

Documentation

Web API

Contents

1	Overview	6
2	Contact Myra	7
3	Security	8
3.1	Generate a signing string	8
3.2	Generate a signing key	9
3.3	Generate a signature	9
3.4	References	10
4	Object descriptions	11
4.1	Objects returned	11
4.1.1	QueryVO	11
4.1.2	ResultVO	11
4.1.3	ViolationVO	12
5	Domain	13
5.1	Overview	13
5.2	Usage	13
5.2.1	Listing	13
5.2.2	Create	14
5.2.3	Update	15
5.2.4	Delete	16
5.3	Full version of a Domain object	17
6	DNS	20
6.1	Overview	20
6.2	Usage	20
6.2.1	Listing	21
6.2.1.1	Filtering	22
6.2.2	Create	22
6.2.3	Update	24
6.2.4	Delete	24
6.3	Full version of a DnsRecord object	25
7	Load balance	28
7.1	Overview	28
7.2	Usage	28
7.2.1	Listing	29
7.2.2	Create	30
7.2.3	Update	32
7.2.4	Delete	32

8	Subdomain settings	33
8.1	Overview	33
8.2	Usage	33
8.2.1	Listing	34
8.2.2	Update	36
8.3	Full version of a Subdomain settings object	37
9	Cache	48
9.1	Overview	48
9.2	Usage	48
9.2.1	Listing	49
9.2.2	Create	49
9.2.3	Update	50
9.2.4	Delete	51
9.3	Full version of a Cache object	51
10	CacheClear	54
10.1	Overview	54
10.2	Usage	54
10.2.1	Clear	55
10.2.2	Clear of a whole domain	56
10.2.3	Bulk CacheClear endpoint	57
10.3	Full version of a CacheClear object	58
10.4	Pattern matching	59
11	Redirects	60
11.1	Overview	60
11.2	Usage	60
11.2.1	Listing	61
11.2.2	Create	62
11.2.3	Update	63
11.2.4	Delete	63
11.3	Full version of a Redirect object	64
12	IP filter	66
12.1	Overview	66
12.2	Usage	66
12.2.1	Listing	67
12.2.2	Create	68
12.2.3	Update	69
12.2.4	Delete	69
12.3	Full version of a IPFilter object	70

13 Maintenance	72
13.1 Overview	72
13.2 Usage	72
13.2.1 Listing	73
13.2.2 Create	74
13.2.3 Update	76
13.2.4 Delete	76
13.3 Full version of a Maintenance object	77
14 SSL certificates	80
14.1 Overview	80
14.2 Usage	80
14.2.1 Listing	80
14.2.2 Create	82
14.2.3 Refreshing existing certificates	83
14.2.4 Update	84
14.2.5 Delete	84
14.3 Full version of a SslCertVO object	85
15 Statistics	90
15.1 Overview	90
15.2 Usage	90
15.2.1 Query	90
15.3 StatisticVO	92
15.3.1 StatisticQueryVO	92
15.3.2 Data sources	94
15.3.2.1 Requests	95
15.3.2.2 Traffic	96
15.3.2.3 Other	97
15.3.3 Result	97
16 IP address ranges of Myra	98
16.1 Overview	98
16.2 Usage	98
16.2.1 Listing	99
16.2.2 Create	99
16.2.3 Update	99
16.2.4 Delete	99
16.3 Full version of a IP address range object	100

17 Error Pages	101
17.1 Overview	101
17.2 Usage	101
17.2.1 Listing	102
17.2.2 Fetching	103
17.2.3 Create	104
17.2.4 Update	104
17.2.5 Delete	105
17.3 Structure of the request JSON	105
17.4 Full version of an error page object	106
18 Rate Limit	107
18.1 Overview	107
18.2 Usage	107
18.2.1 Listing	108
18.2.2 Create	109
18.2.3 Update	110
18.2.4 Delete	110
18.3 Full version of rate limit object	111
19 Bind zone file endpoints	112
19.1 Raw bind zone	112
19.2 JSON bind zone	112
20 Interaction with Myra Web API	115
20.1 Terraform Provider	115
20.2 Go client	115
21 Development	116
21.1 MYRA_NOCACHE	116

1 Overview

The web API of Myra is based on REST using the JSON format for the messages. We are supporting programmatic access to almost every operation you can do on our web backend. You can manage your cache settings accordingly to your deployment cycle or change your DNS settings, to name a few.

If you have any questions about the manual or Myra, please do not hesitate to contact us. You will find our contact data in the “Contact Myra” section of this documentation.

2 Contact Myra

General support inquiries	Ticket center	
Support hotline 12/5	Phone (Mo - Fr, 8 am - 8 pm)	+49 89 9 97 40 18 00
Support hotline 24/7 & emergency	Phone	+49 89 9 97 40 18 88
Sales	Phone/email	+49 89 4 14 14 13 45 sales@myrasecurity.com

For quick help with support inquiries by phone, always create a ticket in the Myra app ticket center, which you can access via **Organization > Ticket center**. This allows our IT experts to correctly categorize and process your request.

3 Security

For all REST calls you use your API key¹ to authenticate your user. The whole communication is encrypted via TLS/SSL. To prevent your configuration from man-in-the-middle attacks or phishing attempts it is necessary to add an additional security layer.

For the additional security layer we have added a hashed signature containing a timestamp, which prevents attackers from repeating a call without knowing the secret for a certain period of time.

```
Authorization: MYRA {apiKey}:{signature}  
Date: {date}  
Content-Type: application/json
```

Listing 1: Authorization header

To calculate a signature you first have to concatenate specific request elements to build a string. After building the string you need to generate a signing key and sign your string with your key.

3.1 Generate a signing string

The code examples below are not in any real programming language, but rather in kind of "pseudo-language". They are meant to serve as hints for concrete implementation in user's language of choice.

The specific request elements you need are:

- MD5 hash of your request body
- your request method
- your URI
- the content type, set in your request header
- the date, set in your request header

You concatenate all those elements with a `#` character. In case of a `GET` request, which cannot contain a request body, please use a MD5 hash of an empty string:

```
d41d8cd98f00b204e9800998ecf8427e
```

Please note that the following example contains spaces for readability. Your signing string should not contain any spaces around the `#` character.

¹You will receive your API key from the Myra support team


```
signingString := "d41d8cd98f00b204e9800998ecf8427e"  
+ "#" + "GET"  
+ "#" + "/en/rapi/cacheSetting/www.example.de"  
+ "#" + "application/json"  
+ "#" + "2014-04-26T13:04:00+0100"
```

3.2 Generate a signing key

A signing key is generated in two steps. First step is to create a date key as hex hmac representation, which is created from the current date and your secret.

```
/**  
 * For example, if: secret is: 6b3a71954faf11e4b898001517fa8424  
 * then dateKey will be 1c2a270750de0cc1b8c3522494abd9a04e0b7801be6ece02755fa7bc9f8f5467  
 */  
dateKey := hmac_sha256("2014-04-26T13:04:00+0100", "MYRA" + secret)
```

Please note: You have to use the same date string as used in the date of your request header where the time is not allowed to differ more than 10 seconds into the future or 30 minutes into the past.

Second step is to use your date key to sign the string 'myra-api-request', which is also created as hex hmac representation.

```
/**  
 * Calculated signingKey will be: 3744ae9c3d3f87c3ce90a99957f9f054266ef9386fc909e2a24a7031c7571ffd  
 */  
signingKey := hmac_sha256("myra-api-request", dateKey)
```

3.3 Generate a signature

To generate a signature you first have to create a signing string and a signing key. After you generated both keys you have to use the signing key to encrypt the signing string via hmac `sha512` and return a `base64` representation of the generated hash.

Please note: the hmac sha512 result is used in binary representation.

```
/**  
 * Calculated signature will be:  
 * 70XCjTTssU9DD/mkbhyp5Syup0ufUm1Y0WUj66hsxmTctVordMIVLS30pi7CSp1hC7EcZ2q1hvpXJMMNkvAncw==  
 */  
signature := base64(hmac_sha512(signingString, signingKey))
```

Finally, here are the steps, in order, to build the required HTTP header:

1. Generate a string to sign

```
signingString := md5(requestBody)
+ "#" + requestMethod
+ "#" + requestUri
+ "#" + requestHeaderData["Content-Type"]
+ "#" + requestHeaderData["Date"]
```

2. Generate signing key

```
dateKey := hmac_sha256(headerDate, "MYRA" + secret)
signingKey := hmac_sha256("myra-api-request", dateKey)
```

3. Build signature

```
signature := base64_encode(hmac_sha512(signingString, signingKey))
```

4. Add to request header

```
Authorization: MYRA $apiKey:$signature
```

3.4 References

- [Go client library](#): Our Go client has a simple interface where you only need to provide your API Key and API secret – the rest is managed by the client automatically.
- [Go Signature repo](#): Go package for generating/adding the required authentication information to a Myra API call.

4 Object descriptions

4.1 Objects returned

All API calls will return an HTTP response code of 200 with one of two different object types or in the error case an appropriate HTTP error code.

A GET call will always return an object of the type QueryVO (Query Value Object) and all other calls return an object from the type ResultVO (Result Value Object).

Each object has similar structured objects, which contain data from the current call.

4.1.1 QueryVO

An object of the type QueryVO is always returned when receiving a list of objects from an API call.

```
{
  "error"   : false,
  "list"    : [],
  "page"    : 1,
  "count"   : 1,
  "pageSize": 50
}
```

Attribute	Type	Description
error	Boolean	Shows if the request had an error
list	Array	A list of matches for the given page
page	Integer	Number of the current page
count	Integer	Number of hits
pageSize	Integer	Number of matches maximal shown at a page

4.1.2 ResultVO

An object of the type ResultVO is always returned for API calls doing inserts, updates, or deletes.

```
{
  "error"           : false,
  "violationList"  : [],
  "targetObject"   : []
}
```

Attribute	Type	Description
error	Boolean	Shows if the request has an error
violationList	Array	A list of ViolationVOs to show validation errors
targetObject	Array	Returns a list of processed objects

4.1.3 ViolationVO

An object of the type ViolationVO (Violation Value Object) shows the exact error for a specific attribute or a generic error if no path is set.

```
{
  "path"   : "",
  "message" : ""
}
```

Attribute	Type	Description
path	String	The attribute name which was not correctly validated
message	String	An error message, which describes what was going wrong

5 Domain

5.1 Overview

You can manage your domains directly with Myra.

5.2 Usage

All domain requests use URL specific parameters; a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
page	Number	Yes	Number of the page you want to retrieve (1-based).

5.2.1 Listing

The listing operation returns a list of domains. The list contains domains for the account you are accessing the API with. The listing returns also additional status information about maintenance, pause, or ownership.

The REST request must have the following format:

```
GET /{language}/rapi/domains/{page} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```

A successful call will return a response with a HTTP status code of 200 and the following body:

```
{
  "error" : false,
  "list" : [
    {
      "objectType" : "DomainVO",
      "name" : "example.com",
      "organizationId" : 1,
      "autoUpdate" : true,
      "maintenance" : false,
      "paused" : true,
      "pausedUntil" : "2023-09-30T14:00:00+0200",
      "dnsRecords" : [],
      "reversed" : false,
      "environment" : "live",
      "locked" : false,
      "id" : 1,
      "modified" : "2013-12-13T11:30:00+0100",
      "created" : "2013-12-09T11:30:00+0100",
      "label" : "example.com"
    }
    ...
  ],
  "page" : 1,
  "count" : 100,
  "violationList" : [],
  "warningList" : [],
  "pageSize" : 50
}
```

5.2.2 Create

To create a new domain it is necessary to send a Domain object without the attributes "id" and "modified". Both attributes will be generated by the server and returned after a successful insert is done.

```
PUT /{language}/rapi/domains HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "name" : "example.com",
  "autoUpdate" : false,
  "autoDns" : false
}
```

A successful insert will return a ResultVO with the new created Domain object:

```
{
  "error" : false,
  "violationList" : [],
  "warningList" : [],
  "targetObject" : [
    {
      "objectType" : "DomainVO",
      "name" : "example.com",
      "organizationId" : 1,
      "autoUpdate" : false,
      "maintenance" : false,
      "paused" : false,
      "dnsRecords" : [],
      "reversed" : false,
      "environment" : "live",
      "locked" : false,
      "id" : 1,
      "modified" : "2013-12-13T11:30:00+0100",
      "created" : "2013-12-09T11:30:00+0100",
      "label" : "example.com"
    }
  ]
}
```

After a successful insert your configuration will be queued and deployed to our system.

5.2.3 Update

Updating a domain is very similar to creating a new one. The main difference is that an update will need the generated **"id"** and **"modified"** attributes to identify the object you are trying to update.

Updating a domain allows you **only to change** some attributes:

- the **autoUpdate** flag,
- the **pause** flag as false,
- the **pause** flag as true and the **pausedUntil** flag with date.

All other values are ignored. If a domain **contains a typo** you have to **remove and recreate** the domain with the correct name.

```
POST /{language}/rapi/domains HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "id" : 3,
  "modified" : "2013-12-09T11:30:00+0100",
  "autoUpdate" : true,
  "paused" : true,
  "pausedUntil" : "2024-09-28T15:00:00+02:00"
}
```

A successful update will return the same type of object as the create operation. After an update your configuration will be queued and deployed to our system.

5.2.4 Delete

For deleting a domain it is only necessary to send the "id" attribute as body content.

Deleted domains are soft deleted and they can be returned. Please contact Myra support if needed.

Removing a domain also removes all configurations on Myra! This could lead to an outage of your online presence. Please make sure that you are prepared for it. If unsure, contact Myra support.

```
DELETE /{language}/rapi/domains HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "id" : 3
}
```

After a delete operation your configuration will be queued and removed from our system.

5.3 Full version of a Domain object

```
{
  "id" : 1,
  "objectType": "DomainV0",
  "organizationId": 175,
  "dnsRecords": [],
  "reversed": false,
  "environment": "live",
  "locked": false,
  "modified" : "2014-03-12T18:21:49+0100",
  "created" : "2014-03-06T18:21:49+0100",
  "name" : "example.com",
  "autoUpdate" : false,
  "autoDns" : false,
  "paused" : true,
  "pausedUntil" : "2014-04-01T00:00:00+0100",
  "maintenance" : false,
  "label": "19111981.de"
}
```

Attribute name	Short description	Type	Supported methods	Required
id	Id of the object	Number	Update, Delete	Yes
modified	Date of last modification	Date	Update	Yes
created	Date of creation	Date	None	No
name	Domain name	String	Create	Yes
autoUpdate	Auto update flag for the domain	Boolean	Create, Update	Optional
autoDns	Auto DNS flag for the domain	Boolean	Create, Update	Optional
paused	Shows if Myra is paused for this domain	Boolean	Create, Update	Optional
pausedUntil	Date until Myra will be automatically reactivated	Date	Create, Update	Optional
maintenance	Shows if this domain is currently on maintenance	Boolean	Create, Update	Optional
objectType	Object type indicator	String	None	No
organizationId	Id of the organisation owning this domain	Number	None	No
dnsRecords	Deprecated, was showing the DNS records of the domain	Array	None	No

Attribute name	Short description	Type	Supported methods	Required
reversed	Shows if the domain is of the type reversed	Boolean	Create, Update	Optional
environment	Type of environment for the domain	String	None	No
locked	Shows if the domain is locked	Boolean	Create, Update	Optional
label	Equivalent to name but without additional normalization	String	None	No

id Id is an unique identifier for an object. This value is always a number type and cannot be set while inserting a new object. To update or delete a Domain it is necessary to add this attribute to your object.

modified Identifies the version of the object. To ensure that you are updating the most recent version and not overwriting other changes, you always have to add modified for updates and deletes. This value is always a date type with an ISO 8601 format

created Created is a date type attribute with an ISO 8601 format. It will be created by the server after creating a new Domain object. This value is informational so it is not necessary to add this attribute to any API call.

name Identifies the domain by its name. The value cannot be changed after creation. To change a typo you need to delete and recreate the domain.

autoUpdate Shows if the current domain has autoUpdate activated. If autoUpdate is deactivated changes on your configuration are not deployed until you reactivate autoUpdate. This is primarily used to change a lot of settings at once to prevent Myra from deploying a half done configuration. In some cases Myra support also deactivates this option to prevent Myra system from removing special configuration settings. Please note that turning autoUpdate off is not correlated to database transactions. This means that any change made are saved but not deployed.
Default value: `true`

autoDns If autoDns flag is set while creating a new domain Myra tries to get a list of subDomains for this domain. Depending on your DNS provider configuration this may fail or return a incomplete list. For best results Myra recommends to use the subDomain API to create DNS records.
Default value: `false`

paused	Shows if the domain is currently in pause mode. Default value: <code>false</code>
pauseUntil	Shows the date when Myra protection will be reactivated automatically. This value is always a date type with an ISO 8601 format.
maintenance	True if this domain is currently in maintenance mode. Maintenance pages can be configured using the Maintenance API. Default value: <code>false</code>
objectType	Shows the object type which is Domain Value Object in this case.
organizationId	Shows the organization ID of the organization owning this domain in the system.
dnsRecords	Deprecated value showing only an empty array, kept for backward compatibility. For DNS records use section 6. DNS Records.
reversed	A boolean showing if the domain in reverse domain name notation. Default value: <code>false</code>
environment	Shows the state environment of the domain. Switching to the test environment allows you to test single features. It is also possible to configure new subdomains and test them before going live.
locked	Shows if the domain is locked in the system. This is different from deleted functionality. Default value: <code>false</code>
label	Equivalent to name but without additional normalization.

6 DNS

6.1 Overview

The DNS settings let you configure your DNS related settings like changing your origin IP or setting up a new DNS record.

6.2 Usage

All DNS requests use URL specific parameters, a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	String	Yes	The domain you are trying to list DNS entries for.
page	Number	Yes	Number of the page you want to retrieve (1-based).

6.2.1 Listing

To list all DNS objects belonging to a given domain you have to use the following REST request:

```
GET /{language}/rapi/dnsRecords/{domain}/{page} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```

A successful call will return a response with a HTTP status code 200 and the following body:

```
{
  "error": false,
  "list": [
    {
      "objectType": "DnsRecordV0",
      "id": 1,
      "modified": "2018-02-02T10:27:25+0100",
      "created": "2018-02-02T10:26:08+0100",
      "name": "subdomain.example.de",
      "value": "127.0.0.1",
      "priority": 0,
      "ttl": 300,
      "recordType": "A",
      "active": true,
      "enabled": true,
      "paused": false,
      "upstreamOptions": {
        "backup": false,
        "down": false
      },
      "alternativeCname": "subdomain-example-de.ax4z.com.",
      "caaFlags": 0,
      "endpoints": [],
      "serviceType": 2
    }
  ],
  "page": 1,
  "count": 11,
  "pageSize": 50
}
```

6.2.1.1 Filtering

The DNS listing endpoint allows to filter the output by using the following URI parameters:

Parameter	Type	Description	Default value
search	String	Filter the DNS records with the specific string in the name or in the value field.	null
recordTypes	String	Filter the DNS by record type. It is possible to specify more than one record type as a comma separated list.	null
activeOnly	Boolean	When set to <code>true</code> only active DNS records are returned.	false
loadbalancer	Boolean	When set to <code>true</code> only returns the DNS records that are being load balanced.	false

6.2.2 Create

The property `sslCertTemplate` is optional. If you do not want to use SSL certificate from an existing subdomain, then just remove the whole property from the request.

To create a new DNS entry you have to send a `DnsRecord` object without the attributes `id`, `created`, and `modified`. All attributes are generated by the server and returned after that.

```
PUT /{language}/rapi/dnsRecords/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "name": "www.example.com",
  "value": "127.0.0.1",
  "ttl": 300,
  "recordType": "A",
  "active": true,
  "sslCertTemplate": "ssldomain.example.com"
}
```

A successful insert will return a ResultVO with the newly created DnsRecord and all records which are matching the same name:

```
{
  "error": false,
  "violationList": [],
  "warningList": [],
  "targetObject": [
    {
      "id": 1,
      "modified": "2014-03-06T18:21:49+0100",
      "created": "2014-03-06T18:21:49+0100",
      "name": "www.example.com",
      "value": "127.0.0.1",
      "priority": 0,
      "ttl": 300,
      "recordType": "A",
      "active": false,
      "paused": false,
      "upstreamOptions": {
        "weight": 1,
        "maxFails": 100,
        "failTimeout": "1",
        "backup": false,
        "down": false,
        "id": 6,
        "modified": "2023-09-13T10:42:47+0200",
        "created": "2023-09-13T10:42:47+0200"
      },
      "alternativeCname": "www-example-com.ax4z.com.",
      "caaFlags": 0,
      "endpoints": [],
      "serviceType": 1,
      "id": 1051446,
      "enabled": true
    }
  ]
}
```

After a successful insert your configuration will be queued and deployed to our system.

6.2.3 Update

Updating a DNS record is very similar to creating a new one. You will need to provide the generated `id` and `modified` attributes to identify the version of object you are trying to update.

```
POST /{language}/rapi/dnsRecords/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "id": 3,
  "name": "www.example.com",
  "value": "127.0.0.2",
  "ttl": 300,
  "recordType": "A",
  "active": true,
  "modified": "2013-12-09T11:30:00+0100"
}
```

To see a valid response, take a look at the response from the create section. After an update your configuration will be queued and deployed to our system.

6.2.4 Delete

To delete a DNS record it is only necessary to send only `id` as body content to identify the version of the record you are trying to delete.

```
DELETE /{language}/rapi/dnsRecords/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "id": 3
}
```

After a delete operation your configuration will be queued and deployed to our system.

6.3 Full version of a DnsRecord object

```
{
  "id": 1,
  "modified": "2014-03-06T18:21:49+0100",
  "created": "2014-03-06T18:21:49+0100",
  "name": "www.example.com",
  "value": "127.0.0.1",
  "priority": 0,
  "ttl": 300,
  "recordType": "A",
  "active": false,
  "enabled": true,
  "paused": false,
  "upstreamOptions": {
    "weight": 1,
    "maxFails": 100,
    "failTimeout": "1",
    "backup": false,
    "down": false,
    "id": 6,
    "modified": "2023-09-13T10:42:47+0200",
    "created": "2023-09-13T10:42:47+0200"
  },
  "alternativeCname": "www-example-com.ax4z.com.",
  "caaFlags": 0,
  "caaTag": "issue",
  "endpoints": [],
  "serviceType": 1,
  "weight": 13
}
```

Attribute name	Short description	Type	Supported methods	Required
id	Id of the object	Integer	Update, Delete	Yes
modified	Date of last modification in ISO 8601 format	Date	Update	Yes
created	Date of creation in ISO 8601 format	Date	-	No
name	Subdomain name of a DNS record	String	Create, Update	Yes
ttl	Time to live	Integer	Create, Update	Optional
recordType	A recordType to identify the type of a record. Valid types are: A , AAAA , MX , CNAME , TXT , NS , and SRV	String	Create, Update	Yes

Attribute name	Short description	Type	Supported methods	Required
sslCertTemplate	A FQDN in the same domain. Default is <code>null</code>	String, Null	Create	Optional
alternativeCname	The alternative CNAME that points to the record.	String	-	-
active	Define whether this subdomain should be protected by Myra or not. Default is <code>false</code>	Boolean	Create, Update	Optional
value	For an <code>A</code> record you use an IPv4 address, for <code>AAAA</code> an IPv6 address, for <code>CNAME</code> a domain name, for <code>MX</code> a domain name (no IP), for <code>NS</code> an IP, for <code>SRV</code> a domain name, and for <code>TXT</code> an arbitrary text.	String	Create, Update	Yes
priority	Priority of <code>MX</code> records	Integer	Create, Update	Optional
paused	<code>True</code> if the DNS record should be disabled (paused) for some-time for maintenance or testing	Boolean	Create, Update	Optional
upstreamOptions	Explained in Load balance section	Object	Create, Update	Optional
caaTag	This lets you choose one of the following: <ul style="list-style-type: none"> - issue: The CA is authorized to provide a certificate for this domain - issuewild: the CA can issue wildcard certificates for this domain - iodef: URL that the CA can use to send an error message, using the Incident Object Description Exchange Format. 	String	Create, Update	Optional

Attribute name	Short description	Type	Supported methods	Required
caaFlags	The default is 0. If you put 1, this blocks the validation if the tag is unknown by the CA.	Integer	Create, Update	Optional
endpoints	This provides the public Myra IPv4/IPv6 addresses for the DNS record	Array	Create, Update	Optional
serviceType	Describes the type of the service behind this DNS record 1 → HTTP 2 → MAIL 3 → OTHER	Integer	Create, Update	Optional
enabled	This specifies if the DnsRecord is enabled or disabled. Default is true	Boolean	Create, Update	Optional
port	Server port on SRV records	Integer	Create, Update	Optional
weight	Weight of that SRV record	Integer	Create, Update	Optional

7 Load balance

7.1 Overview

The load balance setting lets you configure the way different IP addresses pointing to the same DNS record name behave.

7.2 Usage

It is possible to retrieve or modify the load balance settings by using the DNS record endpoint.

All the load balance requests use URL specific parameters, a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	String	Yes	The domain you are trying to list DNS entries for.
page	Number	Yes	Number of the page you want to retrieve (1-based).

7.2.1 Listing

To list all load balance objects belonging to a given domain you have to use the DNS record endpoint by specifying the `loadbalancer=true` filter:

```
GET /{language}/rapi/dnsRecords/{domain}/{page}?loadbalancer=true&recordTypes=A,AAAA,CNAME HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```

A successful call will return a response with a HTTP status code of 200 and the following body:

```
{
  "error": false,
  "list": [
    {
      "objectType": "DnsRecordVO",
      "id": 2,
      "modified": "2018-02-02T10:27:25+0100",
      "created": "2018-02-02T10:26:08+0100",
      "name": "subdomain.example.de",
      "value": "127.0.0.1",
      "priority": 0,
      "ttl": 300,
      "recordType": "A",
      "active": true,
      "enabled": true,
      "paused": false,
      "upstreamOptions": {
        "backup": false,
        "down": false,
        "failTimeout": 3
        "maxFails": 2
        "weight": 2
      },
      "alternativeCname": "subdomain-example-de.ax4z.com.",
      "caaFlags": 0,
      "endpoints": [],
      "serviceType": 2
    },
    ...
  ],
  "page": 1,
  "count": 11,
  "pageSize": 50
}
```

7.2.2 Create

To create a new loadbalance entry, you have to create a `DnsRecord` object without the attributes `id`, `created`, and `modified` but with the same name field as the record is being balanced. All attributes are generated by the server and returned after that. The DNS record end-point allows to specify load balancing settings within the `upstreamOptions` field. The `upstreamOptions` field is an object containing the following fields:

Field name	Short description	Type	Supported methods	Required
weight	Defines the priority for the origin server, the higher the number, the higher the priority of the server. Accepted values: 1 - 2147483648. Default value: 1	Integer	Create, Update	Optional
maxFails	Sets the number of unsuccessful attempts to communicate with the origin that should happen in the duration set by the <code>failTimeout</code> parameter to consider the origin unavailable for a duration also set by the <code>failTimeout</code> parameter. Accepted range: 0 - 2147483648. Default value: 100	Integer	Create, Update	Optional
failTimeout	The time during which the specified number of unsuccessful attempts to communicate with the origin should happen to consider the origin unavailable and the period of time the origin will be considered unavailable. Default value: 1	Integer	Create, Update	Optional
backup	Marks the origin server as backup. The servers marked as backup will receive the requests when the primary servers are unavailable. Default value: <code>false</code>	Boolean	Create, Update	Optional
down	Marks the origin server as permanently unavailable. Default value: <code>false</code>	Boolean	Create, Update	Optional

```
PUT /{language}/rapi/dnsRecords/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}

{
  "name": "www.example.com",
  "value": "1.1.1.2",
  "ttl": 300,
  "recordType": "A",
  "active": true,
  "upstreamOptions": {
    backup: true,
    down: false,
    failTimeout: 3,
    maxFails: 2,
    weight: 2
  }
}
```

A successful insert will return a ResultVO with the newly created DnsRecord and all records which are matching the same name.

7.2.3 Update

Updating a load balanced DNS record is very similar to creating a new one. You will need to provide the generated `id` and `modified` attributes to identify the version of object you are trying to update.

```
POST /[language]/rapi/dnsRecords/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}

{
  "id": 2,
  "modified": "2018-02-02T10:27:25+0100",
  "name": "www.example.com",
  "value": "1.1.1.2",
  "ttl": 300,
  "recordType": "A",
  "active": true,
  "upstreamOptions": {
    backup: true,
    down: false,
    failTimeout: 3,
    maxFails: 2,
    weight: 2
  }
}
```

To see a valid response, take a look at the response from the create section. After an update your configuration will be queued and deployed to our system.

7.2.4 Delete

To delete a DNS record it is only necessary to send `id` as body content. See example to delete DNS record (section 6.2.4).

8 Subdomain settings

8.1 Overview

The subdomain settings API lets you adjust the Myra configuration for your domain or specific subdomains. In the text further the keyword `subdomain` will be used but meaning both subdomain or domain.

8.2 Usage

All subdomain settings requests use URL specific parameters; a list of these parameters can be found in the table below. For subdomain settings you cannot delete or create settings, only update and list them. In case a setting is not set, it takes the default value or the value of the domain settings or the tag settings if a tag is assigned to it.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
subdomain	String	Yes	The subdomain you are trying to list subdomain settings for. Not required if <code>domainId</code> is provided.
domain	Integer	Yes	The domain Id you are trying to list domain settings for. Not required if subdomain is provided.

8.2.1 Listing

To list all subdomain settings objects belonging to a given domain or subdomain, below urls can be used with `domainId` or `subdomainName`:

domainId `/language/rapi/subdomainSetting/domainId`

subdomainName `/language/rapi/subdomainSetting/subdomainName`

A successful call will return a response with a HTTP status code of 200 and the following body:

```
{
  error : false,
  violationList : [],
  domain : {
    "cdn" : true,
    "access_log" : false,
    ...
  },
  targetObject : {
    "hsts_include_subdomains" : false,
    ...
  },
  tag : {
    "hsts" : false,
    ...
  },
  parent : {
    "access_log" : false,
    "antibot" : no,
    "myra_ssl_header" : false,
    "request_limit_level" : 6000,
    ...
  }
}
```

Additionally you can request a already merged representation of the subdomain settings by sending the query parameter `flat`. The result returned will be a flat object with all subdomain specific and inherited settings merged correctly.

```
GET /{language}/rapi/subdomainSetting/{domain}?flat HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```

Example response listing subdomain settings object:

```
{
  "cdn" : true,
  "access_log" : false,
  "antibot" : no,
  "myra_ssl_header" : false,
  "request_limit_level" : 6000,
  ...
}
```

8.2.2 Update

To update a subdomain settings you have to send a subdomain settings object. All attributes are generated by the server and returned after that.

```
POST /{language}/rapi/subdomainSetting/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "access_log" : false,
  "antibot" : "auto",
  "cdn" : true,
  "image_optimization" : false,
  "request_limit_block" : false,
  "rewrite" : "no",
  "security_level" : "high",
  "spdy" : true
}
```

A successful insert will return a ResultVO with the newly created subdomain settings and all settings which are matching the same name.

```
{
  "error": false,
  "violationList": [],
  "targetObject": [
    {
      "access_log" : false,
      "antibot" : "auto",
      "cdn" : true,
      "image_optimization" : false,
      "request_limit_block" : false,
      "rewrite" : "no",
      "security_level" : "high",
      "spdy" : true
    }
  ]
}
```

After a successful update your configuration will be queued and deployed to our system.

8.3 Full version of a Subdomain settings object

The subdomain settings object contains three possible properties `[parent, targetObject, domain]`. The settings for the given subdomain are listed in `domain`. All inherited settings are listed in `parent`. Settings in `domain` always overwrite the inherited setting with the same name. The `targetObject` has a more detailed setting inheritance map.

```
{
  "error": false,
  "targetObject": [
    {
      "accept_encoding": [
        "https",
        "http"
      ],
      "access_log": false,
      "antibot_post_flood": false,
      ...
    },
    {
      "balancing_method": "cookie_based",
      ...
    },
    ...
  ],
  "violationList": [],
  "domain": {
    "only_https": true,
    ...
  },
  "parent": {
    "accept_encoding": [
      "https",
      "http"
    ],
    ...
  }
}
```

Attribute name	Short description	Type	Supported methods	Required
access_log	Activate separated access log	Boolean	Update	Optional
antibot	JavaScript based bot detection	Boolean	Update	Optional
antibot_threshold	Ratio of uncached to cached requests	Number	Update	Optional
balancing_method	Specifies with which method requests are balanced between upstream servers	String	Update	Optional
block_not_whitelisted	Block all IPs, which are not allowlisted	Boolean	Update	Optional
cache_enabled	Turn caching on or off	Boolean	Update	Optional
cache_revalidate	Enable stale cache item revalidation	Boolean	Update	Optional
cdn	Use subdomain as Content Delivery Node (CDN)	Boolean	Update	Optional
client_max_body_size	Maximum client request body size	Integer	Update	Optional
cookie_name	Cookie name for cookie based load balancing	String	Update	Optional
diffie_hellman_exchange	The Diffie-Hellman key exchange parameter length	Integer	Update	Optional
disable_forwarded_for	Disable X-Forward for directive	Boolean	Update	Optional
host_header	Set the host header	String	Update	Optional
hsts	HSTS Strict Transport Security (HSTS)	Boolean	Update	Optional
hsts_include_subdomains	HSTS includeSubDomains directive	Boolean	Update	Optional
hsts_max_age	HSTS max-age	Number	Update	Optional
hsts_preload	HSTS preload directive	Boolean	Update	Optional
http_origin_port				

Attribute name	Short description	Type	Supported methods	Required
forwarded_for_replacement	Set your own X-Forwarded-For header	String	Update	Optional
image_optimization	Optimization of images	Boolean	Update	Optional
ipv6_active	Allow connections via IPv6 to your systems	Boolean	Update	Optional
myra_ssl_header	Activates the X-Myra-SSL header	Boolean	Update	Optional
next_upstream	Specifies the error that mark the current upstream as down	String	Update	Optional
only_https	Shall the origin server always be requested via HTTPS	Boolean	Update	Optional
origin_connection_header	Connection header	String	Update	Optional
proxy_cache_bypass	Name of the cookie which forces Myra to deliver the response not from cache	String	Update	Optional
proxy_cache_stale	Determines in which cases a stale cached response can be used when an error occurs	String	Update	Optional
proxy_connect_timeout	Timeout for establishing a connection to the upstream server	Number	Update	Optional
proxy_read_timeout	Timeout for reading the upstream response	Number	Update	Optional

Attribute name	Short description	Type	Supported methods	Required
request_limit_block	Show CAPTCHA after exceeding the configured request limit	Boolean	Update	Optional
request_limit_level	Sets how many requests are allowed from an IP per minute	Number	Update	Optional
rewrite	Enable the JavaScript optimization	String	Update	Optional
rewrite_regex	Regular Expression to match the JavaScript files to optimize	String	Update	Optional
security_level	Activate Web Application Filter	String	Update	Optional
spdy	Activates the SPDY protocol	Boolean	Update	Optional
streaming_regex	Regular expression to match the streaming URL	String	Update	Optional

access_log

Activate separated access log. A access log from each Myra node delivering your website will be saved. You can download the access log files via sftp from custlogs.myracloud.com.

Default value: `false`

Allowed values: `true`, `false`

antibot

Activate JavaScript based bot detection. Bots will then be automatically blocked when accessing your website.

Default value: `no`

Allowed values: `yes`, `no`, `auto`

antibot_threshold

(Advanced) Sets the ratio of uncached to cached requests. This options is only used when Antibot is set to "auto".

Default value: `20`

Allowed values: `0 - 100`

balancing_method

Specifies with which method requests are balanced between upstream servers. The default behavior is the round-robin balancing. The value `ip_hash` will cause Myra to forward the same client IP always to the same

	<p>upstream server. The value <code>least_conn</code> will cause Myra to forward the request to the upstream server with least connections.</p> <p>Default value: <code>round_robin</code></p> <p>Allowed values: <code>round_robin</code>, <code>ip_hash</code>, <code>least_conn</code>, <code>cookie_based</code></p>
block_not_whitelisted	<p>Block all IPs which are not allowlisted in the IP filter settings.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
cache_enabled	<p>Turn caching on or off. If you enable the cache, you also have to define the objects to be cached in the cache settings.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
cache_revalidate	<p>If enabled, expired cache items will be requested with the additional HTTP header "If-Modified-Since" and "If-None-Match".</p> <p>Default value: <code>true</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
cdn	<p>(Advanced) Should this subdomain be used as Content Delivery Node (CDN). After enabling the CDN you will be able to create buckets and upload files using the Myra upload API.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
client_max_body_size	<p>Sets the maximum allowed size of the client request body, specified in the "Content-Length" request header field. Maximum 5120 MB.</p> <p>Default value: <code>10 MB</code></p>
cookie_name	<p>When <code>cookie_based</code> is selected for balancing method, a cookie name should also be provided.</p>
diffie_hellman_exchange	<p>Defines the size of the Diffie-Hellman key exchange parameters in bits. Please, note that Java 6 and 7 do not support Diffie-Hellman parameters larger than 1024 bits. If your server expects to receive connections from</p>

	<p>java 6 clients and wants to enable PFS, it must provide a DHE parameter of 1024 bits.</p> <p>Default value: <code>1024</code></p> <p>Allowed values: <code>1024</code>, <code>2048</code></p>
disable_forwarded_for	<p>Disable X-Forward for directive.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
enforce_cache_ttl	<p>(Advanced) Enforce using given cache TTL settings instead of origin cache information. This will set the Cache-Control header max-age to the given TTL.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
host_header	<p>Set a specific host header.</p> <p>Default value: <code>\$myra_host</code></p>
hsts	<p>(Advanced) Enable HSTS protection for a domain. This will tell browsers to use secure https connections only when interacting with your domain.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
hsts_include_subdomains	<p>(Advanced) This will extend the HSTS protection for all subdomains.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
hsts_max_age	<p>(Advanced) Specified how long the HSTS header is valid before the browser has to revalidate.</p> <p>Default value: <code>31536000</code></p> <p>Allowed values: <code>0</code> - <code>2147483647</code></p>
hsts_preload	<p>(Advanced) Allow the domain to be added to the HSTS preload list used by all major browsers (https://hstspreload.appspot.com/).</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
forwarded_for_replacement	<p>Set your own X-Forwarded-For header. The value of this header contains the originating IP address of the request.</p> <p>Default value: <code>X-Forwarded-For</code></p> <p>Allowed values: A valid HTTP header name</p>

image_optimization	<p>Activate lossless optimization of JPEG and PNG images (recommended setting).</p> <p>Default value: <code>true</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
ipv6_active	<p>Allow connections via IPv6 to your systems. IPv4 connections will be forwarded in any case.</p> <p>Default value: <code>true</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
myra_ssl_header	<p>(Advanced) Activate the <code>X-Myra-SSL</code> header, which indicates if a request was received via SSL.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
next_upstream	<p>(Advanced) Specify in which case the current upstream should be marked as "down". The values can be arbitrary combined, expect the value <code>off</code>.</p> <p>Default value: <code>[error, timeout, invalid_header]</code></p> <p>Allowed values: <code>error</code>, <code>timeout</code>, <code>invalid_header</code>, <code>http_500</code>, <code>http_502</code>, <code>http_503</code>, <code>http_504</code>, <code>off</code></p> <p>error, timeout: An generic error or timeout occurred while connecting to the origin server, sending the request or reading the response.</p> <p>invalid_header: Invalid or empty response from the origin server.</p> <p>http_500, http_502, http_503, http_504: Origin server responded with the matching response code.</p> <p>off: Completely disables the next_upstream behavior.</p>
only_https	<p>If activated, Myra will forward all requests to the origin using HTTPS regardless of the used protocol of the originating request.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
origin_connection_header	<p>(Advanced) Sets the Connection header, which is transmitted to the origin with a request.</p> <p>Default value: <code>none</code></p> <p>Allowed values: <code>upgrade</code>, <code>close</code>, <code>none</code></p>
proxy_cache_bypass	<p>(Advanced) Defines the name of the cookie which forces Myra to deliver the response not from cache. The</p>

values of the cookie must be not empty or equal to 0 to enable bypassing.

Default value: `MYRA_NOCACHE`

Allowed values: A string containing only letters, digits and underscores.

proxy_cache_stale

Determines in which cases a stale cached response can be used when an error occurs during communication with your server. The values can be arbitrary combined, expect the value `off`.

Default value: `[updating]`

Allowed values: `error`, `timeout`, `invalid_header`, `updating`, `http_500`, `http_502`, `http_503`, `http_504`, `http_403`, `http_404`, `off`

error, timeout: An generic error or timeout occurred while connecting to the origin server, sending the request or reading the response.

invalid_header: Invalid or empty response from the origin server.

http_500, http_502, http_503, http_504: Origin server responded with the matching response code.

off: Completely disables the next_upstream behavior.

updating: Allows sending a stale cached response while it is being updated to reduce connections to the origin servers.

proxy_connect_timeout

Defines a timeout in seconds for establishing a connection with the origin server. The timeout cannot be greater than 60 seconds.

Default value: `20`

Allowed values: `1 - 60`

proxy_read_timeout

Defines a timeout in seconds for reading a response from the proxied server. The timeout is set only between two successive read operations, not for the transmission of the whole response.

Default value: `1200`

Allowed values: `1 - 1200`

request_limit_block

If activated, the user has to solve a CAPTCHA after exceeding the configured request limit.

	<p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
request_limit_level	<p>Define how many requests are allowed from an IP per minute. If this limit is reached, the IP will be blocked. If <code>request_limit_block</code> is enabled, the user can solve a CAPTCHA to unblock his IP address.</p> <p>Default value: <code>6000</code></p> <p>Allowed values: <code>0</code> - <code>65535</code></p>
request_limit_report	<p>If activated, an email will be send containing blocked ip addresses that exceeded the configured request limit.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
rewrite	<p>(Advanced) Enable automated JavaScript optimization. All JavaScript is collected and executed at the end of the page. This significantly decreases the DOM content loaded time. If not all JavaScript files should be collected you can set the value to <code>regex</code> and specify the regex to use while matching filenames in the option <code>rewrite_regex</code>.</p> <p>Default value: <code>no</code></p> <p>Allowed values: <code>yes</code>, <code>no</code>, <code>regex</code></p>
rewrite_regex	<p>(Advanced) Regular Expression which is used to match the JavaScript files which should be optimized. All files not matching this pattern will not be touched. This value will only be used if the option <code>rewrite</code> has the value <code>regex</code>.</p> <p>Default value: (empty)</p> <p>Allowed values: Valid regular expression</p>
security_level	<p>Activate the Web Application Filter to block Layer 7 attacks.</p> <p>Default value: <code>standard</code></p> <p>Allowed values: <code>high</code>, <code>standard</code>, <code>off</code></p>
source_protocol	<p>Define which protocol should be used when passing a request to your servers. The value <code>same</code> will ensure that the same protocol is used as in the originating request to Myra. The <code>http</code> and <code>https</code> value will force Myra to always use the specified protocol when connecting.</p> <p>Default value: <code>same</code></p> <p>Allowed values: <code>same</code>, <code>http</code>, <code>https</code></p>

spdy	<p>Activate the high performance HTTP/2 protocol. Please note that you have to enable HTTPS for Myra to get HTTP/2 enabled.</p> <p>Default value: <code>false</code></p> <p>Allowed values: <code>true</code>, <code>false</code></p>
streaming_regex	<p>(Advanced) Regular expression, which is used to match the streaming URL.</p> <p>Default value: (empty)</p> <p>Allowed values: Valid regular expression</p>
ssl_origin_port	<p>Advanced setting: Allows to set a port for communication with origin via SSL.</p> <p>Default value: <code>443</code></p>
monitoring_contact_email	<p>Email addresses, to which monitoring emails should be send. Multiple addresses are separated with a space.</p> <p>Default value: <code>Null</code></p>
monitoring_alert_threshold	<p>Errors per minute that must occur until a report is sent.</p> <p>Default value: <code>300</code></p>
log_format	<p>Use a different log format. A selection of Myra predefined log formats.</p> <p>Default value: <code>myra-combined-waf</code></p>
ignore_nocache	<p>If activated, no-cache headers (Cache-Control: [private no-store no-cache]) will be ignored.</p> <p>Default value: <code>no</code></p>
cache_revalidate	<p>If enabled, expired cache items will be requested with the additional HTTP header "If-Modified-Since" and "If-None-Match".</p> <p>Default value: <code>no</code></p>
block_tor_network	<p>Block traffic from the TOR network.</p> <p>Default value: <code>no</code></p>
antibot_post_flood	<p>Detection of POST floods by using a JavaScript based puzzle.</p> <p>Default value: <code>no</code></p>
antibot_post_flood_threshold	<p>This parameter determines the frequency how often the puzzle has to be solved. The higher the value the less likely the puzzle needs to be solved.</p> <p>Default value: <code>540</code></p>

hsts_include_subdomains	Include all subdomains in HSTS protection. Default value: <code>no</code>
enable_origin_sni	Enable or disable origin SNI. Default value: <code>yes</code>
waf_enable	Enables or disables the Web Application Firewall (WAF). Default value: <code>no</code>
waf_policy	Default policy for the Web Application Firewall in case of rule error. Default value: <code>allow</code>
waf_levels_enable	Enabled WAF hierarchy, a choice of (tag, domain, sub-domain). Default value: <code>All selected</code>
limit_tls_version	Only selected TLS versions will be used. Default value: <code>TLSv1, TLSv1.1, TLSv1.2, TLSv1.3</code>
ssl_client_verify	Enables verification of client certificates. Default value: <code>off</code>
ssl_client_header_fingerprint	Contains the fingerprint of the certificate, the client used to authenticate itself. Default value: <code>X-MYRA-SSL-Fingerprint</code>
ssl_client_header_verification	The name of the header, which contains the ssl verification status. Default value: <code>X-MYRA-SSL-VERIFIED</code>
request_limit_report_email	Email addresses, to which request limit emails should be send. Multiple addresses are separated with a space. Default value: <code>null</code>

9 Cache

9.1 Overview

The cache settings allows you to configure paths, which should be cached by Myra.

9.2 Usage

All cache settings use URL specific parameters, a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	Number, String	Yes	The <code>domainId</code> or <code>subdomainName</code> of the domain you want to interact with. For global domain settings you can also use <code>ALL-0000</code> where the 0000 is the <code>domainId</code> .
page	Number	Yes	Number of the page you want to retrieve (1-based).

9.2.1 Listing

To list all CacheSetting objects belonging to a given domain you have to use the following REST request:

```
GET /{language}/rapi/cacheSettings/{domain}/{page} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17:00+02:00
```

A successful call will return a response with a HTTP status of 200 and the following body:

```
{
  "error": false,
  "list": [
    {
      "id": 1,
      "modified": "2023-09-08T16:30:00+02:00",
      "created": "2022-12-08T16:30:00+02:00",
      "path": "/",
      "ttl": 300,
      "type": "prefix"
    }
  ],
  "page": 1,
  "count": 2,
  "pageSize": 50
}
```

9.2.2 Create

To create a new CacheSetting you need to send a CacheSetting object without the attributes `id`, `created`, and `modified`. All those attributes are generated by the server and returned to you after a successful insert.

```
PUT /{language}/rapi/cacheSettings/{domain} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17:00+02:00

{
  "path": "/",
  "ttl": 300,
  "type": "prefix"
}
```

A successful insert will return a ResultVO with the newly created CacheSetting returned as in the targetObject list.

```
{
  "error": false,
  "violationList": [],
  "targetObject": [
    {
      "id": 1,
      "modified": "2023-09-08T16:30:00+02:00",
      "created": "2022-12-08T16:30:00+02:00",
      "path": "/",
      "ttl": 300,
      "type": "prefix"
    }
  ]
}
```

9.2.3 Update

Updating a CacheSetting is very similar to create a new one. The main difference is that an update will need the `id` and `modified` attributes to identify the version of the object you are trying to update.

```
POST /{language}/rapi/cacheSettings/{domain} HTTP1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17:00+02:00

{
  "id": 1,
  "modified": "2023-09-08T16:30:00+02:00",
  "created": "2022-12-08T16:30:00+02:00",
  "path": "/assets",
  "ttl": 300,
  "type": "prefix"
}
```

To see a valid response, take a look at the response from the create section. After an update your configuration will be queued and deployed to our system.

9.2.4 Delete

To delete a cache rule you only need to send `id` as body content.

```
DELETE /{language}/rapi/cacheSettings/{domain} HTTP1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17:00+02:00

{
  "id": 1
}
```

After a delete operation is done you configuration will be queued and deployed to our system.

9.3 Full version of a Cache object

```
{
  "objectType": "CacheSettingV0",
  "id": 1,
  "modified": "2023-09-08T16:30:00+02:00",
  "created": "2022-12-08T16:30:00+02:00",
  "path": "/",
  "ttl": 300,
  "type": "prefix",
  "not_found_ttl": 300,
  "enforce": true,
  "sort": 3,
  "enabled": true
}
```

Attribute name	Short description	Type	Supported methods	Required
id	Id of the object	Number	Update, Delete	Yes
modified	Date of last modification	Date	Update	Yes
created	Date of creation of the object	Date	None	No
path	Path which must match to the cache response	String	Create, Update	Yes
ttl	Time to live of the object	Number	Create, Update	Yes
type	Type how path should match	String	Create, Update	Yes

Attribute name	Short description	Type	Supported methods	Required
not_found_ttl	How long an object will be cached. Origin responses with the HTTP codes 404 will be cached.	Number	Update	Optional
enforce	Enforce cache TTL allows you to set the cache TTL (Cache Control: max-age) in the backend regardless of the response sent from your Origin.	Boolean	Update	Optional
sort	The order in which the cache rules take action as long as the cache sorting is activated.	Number	Update	Optional
enabled	Define whether this cache setting is enabled or not.	Boolean	Update	Optional

id Id is an unique identifier for an object. This value is always a number type and cannot be set while inserting a new object. To update or delete a cache setting it is necessary to add this attribute to your object.

modified Identifies the version of the object. To ensure that you are updating the most recent version and not overwriting other changes, you always have to add the modified timestamp for updates and deletes. This value is always a date type with an ISO 8601 format.

created Created is a date type attribute with an ISO 8601 format. It will be created by the server after creating a new cache setting object. This value is only informational so it is not necessary to add this an attribute to any API call.

path A request will be matched against this path to decide if this request is cacheable or not. It is possible to write a regexp in this attribute. It is not allowed to use start '^' or end '\$' regexp characters as it they are generated depending on the given type.

ttl Time to live limits the lifespan of a cached response for the given path. This is a numeric value and is given in seconds. Special case is 'like origin server', which uses the TTL returned by your origin server.

not_found_ttl How long an object will be cached. Origin responses with the HTTP codes 404 will be cached.
Default value: 60

enforce	<p>Enforce cache TTL allows you to set the cache TTL (Cache Control: max-age) in the backend regardless of the response sent from your Origin. Attention: Enforce cache TTL is not applied in case of a no-cache rule such as Cache-Control: (no-store no-cache private) or Cache-Control: max-age=0.'</p> <p>Default value: <code>false</code></p>
type	<p>This attribute helps the server to know on how to match the given path against a request.</p> <p>Available options: <code>prefix</code>, <code>suffix</code>, <code>exact</code></p>
sort	<p>The order in which the cache rules take action as long as the cache sorting is activated. Please contact support to change this setting.</p> <p>Default value: <code>0</code></p>
enabled	<p>Define whether this cache setting is enabled or not.</p> <p>Default value: <code>true</code></p>

10 CacheClear

10.1 Overview

CacheClear allows you to delete your cached files on all Myra nodes. You can use wildcard expressions to handle complex clear action as well.

10.2 Usage

All cache clear actions use URL specific parameters; a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	String	Yes	The <code>domainName</code> of the domain you want to interact with.

10.2.1 Clear

To enqueue a clear operation you need to send a CacheClear object. The `fqdn` attribute in the object must be the domain or a subdomain of the domain mentioned in the URL.

```
PUT /{language}/rapi/cacheClear/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "fqdn": "www.example.com",
  "resource": "/*.jpg",
  "recursive": true
}
```

A successfully enqueued cache clear will return a ResultVO with the given CacheClear in the `targetObject` list.

```
{
  "error": false,
  "violationList": [],
  "targetObject": [
    {
      "fqdn": "www.example.com",
      "resource": "/*.jpg",
      "recursive": true
    }
  ]
}
```

10.2.2 Clear of a whole domain

To enqueue a cache clear operation for your complete domain, you have to remove the `fqdn` attribute in the request.

```
PUT /{language}/rapi/cacheClear/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "resource": "/*.jpg",
  "recursive": true
}
```

A successfully queued cache clear will return a ResultVO. For each active subdomain the API returns a CacheClearVO as part of the `targetObject` list. Every CacheClearVO contains the subdomain as `fqdn` attribute and the rest of the given data such as `resource` and `recursive`.

```
{
  "error": false,
  "violationList": [],
  "targetObject": [
    {
      "fqdn": "www.example.com",
      "resource": "/*.jpg",
      "recursive": true
    },
    {
      "fqdn": "www2.example.com",
      "resource": "/*.jpg",
      "recursive": true
    }
  ]
}
```


10.2.3 Bulk CacheClear endpoint

A bulk cache endpoint is used to queue a CacheClear for multiple paths on the specified domain. The clear cache can be defined for a specific subdomain, a specific location or multiple locations, which can be specified with wildcards.

```
PUT /{language}/rapi/cacheClear/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "fqdn": "www.example.com",
  "bulk": [
    "/*.jpg",
    "/*.js"
  ],
  "recursive": true
}
```

A successfully enqueued cache clear will return a ResultVO with the given CacheClear in the targetObject list.

```
{
  "error": false,
  "violationList": [],
  "warningList": [],
  "targetObject": [
    {
      "fqdn": "www.example.com",
      "resource": "/*.js",
      "recursive": true,
      "bulk": [
        "/*.txt",
        "/*.js"
      ]
    }
  ]
}
```

10.3 Full version of a CacheClear object

```
{
  "fqdn": "www.example.com",
  "recursive": true,
  "resource": "/*.jpg",
  "bulk": ["/*.css", "/*.txt"]
}
```

Attribute name	Description	Method type	Required
fqdn	If set, the cache for this subdomain will be cleared. If not set the whole domain will be cache cleared	String	Optional
recursive	Should the pattern also matched against sub-directories	Boolean	Yes
resource	Resource pattern to delete or empty for a full CacheClear	String	Optional
bulk	List of resources to clear, if this is set, the resource attribute will be ignored	Array	Optional

10.4 Pattern matching

Internally we use the `fnmatch` (flags=FNM_PATHNAME) function to find the matching resources that should be deleted. To allow you to do `recursive` deletion in folder, the flag `recursive` was added.

Pattern	Recursive	Resource	Result
/*.js	No	/main.js	match
/*.js	No	/folder/main.js	no match
/*.js	No	/testmain.css	no match
.js	Yes	/assets/script.js	match
.js	Yes	/assets/jquery/jquery.js	match
.js	Yes	/main.js	match
.js	Yes	/main.css	no match
.js	Yes	/assets/js/source.map	no match
/assets/*.js	No	/assets/script.js	match
/assets/*.js	No	/asset/script.js	no match
/assets/*.js	No	/main.js	no match
/assets/*.js	No	/folder/js/script.js	no match
/assets/*.js	Yes	/assets/script.js	match
/assets/*.js	Yes	/assets/jquery/jquery.js	match
/assets/*.js	Yes	/main.js	no match
/assets/*.js	Yes	/js/angular.js	no match
/*.*	Yes	/main.js	match
/*	Yes	/main.js	match

11 Redirects

11.1 Overview

You can manage your redirects directly with Myra, which saves requests to your origin server. The redirect option of Myra offers the possibility of using regular expressions.

11.2 Usage

All redirect requests use URL specific parameters, a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	String	Yes	The domain you are trying to list redirects for.
page	Number	Yes	Number of the page you want to retrieve (1-based).

11.2.1 Listing

The listing operation returns a list of redirects for the given domain. The REST request must have the following format:

```
GET /{language}/rapi/redirects/{domain}/{page} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```

A successful call will return a response with a HTTP status code 200 and the following body:

```
{
  "error": false,
  "list": [
    {
      "id": 1,
      "modified": "2013-12-13T11:30:00+0100",
      "created": "2013-12-13T11:30:00+0100",
      "subDomainName": "www.example.com",
      "source": "/",
      "destination": "$scheme://www.example.com/a.html",
      "type": "redirect",
      "matchingType": "prefix",
      "sort": 0,
      "enabled": true
    }
  ],
  "page": 1,
  "count": 1,
  "pageSize": 50
}
```

11.2.2 Create

To create a new redirect it is necessary to send a Redirect object without the attributes `id` and `modified`. Both attributes will be generated by the server and returned after a successful insert is done.

```
PUT /{language}/rapi/redirects/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}

{
  "source": "/example-source",
  "destination": "http://www.myracloud.com",
  "type": "permanent",
  "matchingType": "prefix",
  "expertMode": false
}
```

A successful insert will return a ResultVO with the new created Redirect object.

```
{
  "error": false,
  "violationList": [],
  "targetObject": [
    {
      "id": 1,
      "modified": "2014-03-06T18:21:49+0100",
      "created": "2014-03-06T18:21:49+0100",
      "subDomainName": "www.example.com",
      "source": "/example-source",
      "destination": "http://www.myracloud.com",
      "type": "permanent",
      "matchingType": "prefix",
      "sort": 0,
      "enabled": true
    }
  ]
}
```

After a successful insert your configuration will be queued to and deployed to our system.

11.2.3 Update

Updating a redirect is very similar to creating a new one. The main difference is that an update will need the generated `id` and `modified` attributes to identify the object you are trying to update.

```
POST /{language}/rapi/redirects/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}

{
  "id": 3,
  "modified": "2013-12-09T11:30:00+0100",
  "source": "/example-source",
  "destination": "http://www.myracloud.com",
  "type": "permanent",
  "matchingType": "suffix",
  "expertMode": false
}
```

A successful update will return the same type of object as the create operation. After an update your configuration will be queued and deployed to our system.

11.2.4 Delete

For deleting a Redirect it is only necessary to send the `id` attribute as body content.

```
DELETE /{language}/rapi/redirects/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}

{
  "id": 3
}
```

After a delete operation your configuration will be queued and deployed to our system.

11.3 Full version of a Redirect object

```
{
  "id": 1,
  "modified": "2014-03-12T18:21:49+0100",
  "created": "2014-03-12T18:21:49+0100",
  "subDomainName": "www.example.com",
  "source": "/example-source",
  "destination": "http://www.myracloud.com",
  "type": "permanent",
  "matchingType": "prefix",
  "sort": 0,
  "enabled": true,
  "expertMode": false
}
```

Attribute name	Short description	Type	Supported methods	Required
id	Id of the object	Number	Update, Delete	Yes
modified	Date of last modification in ISO 8601 format	Date	Update, Delete	Yes
created	Date of creation in ISO 8601 format	Date	None	No
subDomainName	Subdomain of redirect	String	Create, Update	Yes
source	Location to match against	String	Create, Update	Yes
destination	Target where redirect should point to	String	Create, Update	Yes
type	Type of redirect	String	Create, Update	Yes
matchingType	Type to match the redirect defaults to <code>exact</code> .	String	Create, Update	Optional
expertMode	Enable or disable expertMode	Boolean	Create, Update	Optional
sort	The ascending order for the redirect rules	Number	Create, Update	Optional

id Id is an unique identifier for an object. This value is always a number type and cannot be set while inserting a new object. To update or delete a Redirect it is necessary to add this attribute to you object.

modified	Identifies the version of the object. To ensure that you are updating the most recent version and not overwriting other changes, you always have to add modified for updates and deletes. This value is always a date type with an ISO 8601 format.
created	Created is a date type attribute with an ISO 8601 format. It will be created by the server after creating a new Redirect object. This value is only informational so it is not necessary to add this attribute to any API call.
subDomainName	Identifies the subdomain via a FQDN (Full Qualified Domain Name) where this redirect belongs to. This value cannot be changed through the object's attribute as it is set via URL parameter.
source	Location to match your query against, it is also possible to match against a regular expression instead of hard coded location values.
destination	The destination you want your customer redirect to. This can be a valid HTTP(S) address or a relative location on your domain.
type	<p>The redirect type how your customer is redirected. This can be an HTTP 301 (permanent) redirect, which is cacheable by browsers and search crawlers. Another option is an HTTP 302 (redirect) redirect which is usually not cached by browsers and crawlers.</p> <p>Valid options: <code>permanent</code> and <code>redirect</code></p>
matchingType	<p>The matching type allows you to change the way how the redirect is matched.</p> <p>Default value: <code>exact</code></p> <p>Available values: <code>prefix</code>, <code>suffix</code>, <code>exact</code>.</p> <p>prefix: This option places a <code>^</code> in front of your redirect.</p> <p>suffix: The option places a <code>\$</code> at the end of your redirect.</p> <p>exact: The regex will be used like it is without changes.</p>
expertMode	Enable or disable the expertMode. When expertMode is enabled, Myra will skip checking the rule for endless looping.
sort	The ascending order for the redirect rules. The least number has the most priority to be executed. If a couple of rules can be applied to a source, then the rule with least number is taken.

12 IP filter

12.1 Overview

The IP filter of Myra lets you grant or deny access from individual IP addresses or subnets.

12.2 Usage

All IP filter REST calls use URL specific parameters, a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	String	Yes	The domain or subdomain you are trying to list IP filter for.
page	Number	Yes	Number of the page you want to retrieve (1-based).

12.2.1 Listing

To list all IP filter object belonging to a given domain you gave to use the following REST request:

```
GET /{language}/rapi/ipfilter/{domain}/{page} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
```

A successful call will return a response with a HTTP status of 200 and the following body:

```
{
  "error": false,
  "list": [
    {
      "id": 1,
      "modified": "2023-09-11T13:51:58+0200",
      "created": "2023-09-11T13:51:58+0200",
      "subDomainName": "www.example.com",
      "type": "WHITELIST",
      "value": "1.2.3.4/32",
      "enabled": true
    }
  ],
  "page": 1,
  "count": 1,
  "pageSize": 50,
}
```

12.2.2 Create

To create a new IP filter setting, you need to send an `IpFilter` object without the attributes `id`, `created` and `modified`. All those attributes are generated by the server and returned to you after a successful insert.

```
PUT /{language}/rapi/ipfilter/{domain} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
{
  "type" : "BLACKLIST",
  "value" : "1.2.3.4/32"
}
```

A successful insert will return a `ResultVO` with the newly created `IpFilter` object returned in the `targetObject` list.

```
{
  "error": false,
  "violationList": [],
  "warningList": [],
  "list": [
    {
      "id": 1,
      "modified": "2023-09-11T13:51:58+0200",
      "created": "2023-09-11T13:51:58+0200",
      "subDomainName": "www.example.com",
      "type": "BLACKLIST",
      "value": "1.2.3.4/32",
      "enabled": true
    }
  ],
  "page": 1,
  "count": 1,
  "pageSize": 50,
}
```

12.2.3 Update

Updating an IP filter settings is very similar to creating a new one. The main difference is that an update will need the `id` and `modified` attributes to identify the version of the object you are trying to update.

```
POST /{language}/rapi/ipfilter/{domain} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
{
  "id": 1,
  "modified": "2013-12-09T11:30:00+01:00",
  "type" : "WHITELIST",
  "value" : "5.6.7.8/32"
}
```

To see a valid response, take a look at the response from the create section. After an update your configuration will be queued and deployed to our system.

12.2.4 Delete

To Delete a filter rule you only need to send only `id` as body content.

```
DELETE /{language}/rapi/ipfilter/{domain} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
{
  "id": 1
}
```

After a delete operation is done your configuration will be queued and deployed to our system.

12.3 Full version of a IPFilter object

```
{
  "id": 1,
  "modified": "2013-12-09T11:30:00+01:00",
  "created": "2013-12-09T11:30:00+01:00",
  "type" : "WHITELIST",
  "value" : "5.6.7.8/32",
  "enabled": true
}
```

Attribute name	Short description	Type	Supported methods	Required
id	Id of the object	Number	Update, Delete	Yes
modified	Date of last modification	Date	Update	Yes
created	Date of creation	Date	-	No
type	Type of the filter rule	String	Create, Update	Yes
value	Single IPv4 or IPv6 address or CIDR notation	String	Create, Update	Yes
enabled	Shows if the IPFilter is enabled or disabled	Boolean	Create, Update	Optional

id Id is an unique identifier for an object. This value is always a number type and cannot be set while inserting a new object. To update or delete a IPFilter it is necessary to add this attribute to your object.

modified Identifies the version of the object. To ensure that you are updating the most recent version and not overwriting other changes, you always have to add the modified timestamp for updates and deletes. This value is always a date type with an ISO 8601 format.

created Created is a date type attribute with an ISO 8601 format. It will be created by the server after creating a new IPFilter object. This value is only informational so it is not necessary to add this attribute to any API call.

type This specifies how the rule is applied.
Valid values: `WHITELIST`, `BLACKLIST`, `WHITELIST_REQUEST_LIMITER`

value The value of an IPFilter rule can contain a single IP address or a CIDR notation. IPv4 and IPv6 both are supported. If the type is `WHITELIST` or `BLACKLIST`, then the value can be a single or range of IPv4 addresses or single IPv6 address. If the type is `WHITELIST_REQUEST_LIMITER`, then the value can be a single or range of IPv4 or IPv6 addresses.

enabled This specifies if the IPFilter is enabled or disabled.
Default value: `true`

13 Maintenance

13.1 Overview

The maintenance functionality allows you to set a maintenance page which is directly served from Myra servers. This is useful when you are going to maintain your servers and remove all load from your server.

13.2 Usage

For a better user experience, our system will periodically remove all expired maintenance pages.

All maintenance calls use URL specific parameters; a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	String	Yes	The domain you are trying to list maintenance pages for.
page	Number	Yes	Number of the page you want to retrieve (1-based).

13.2.1 Listing

To get a list of all maintenance objects belonging to your given domain you have to use the following REST request:

To list the maintenance pages of a single subdomain replace the domain parameter with your subdomain. This will return only the maintenance pages for the given subdomain.

```
GET /{language}/rapi/maintenance/{domain}/{page} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
```

A successful call will return a response with a HTTP status of 200 and the following body:

```
{
  "error" : false,
  "list" : [
    {
      "id" : 1,
      "modified" : "2013-12-09T11:35:00+0100",
      "created" : "2013-12-09T11:35:00+0100",
      "fqdn" : "www.example.de.",
      "content" : "<html>Your maintenance page</html>",
      "start" : "2013-12-10T00:00:00+0100",
      "end" : "2013-12-10T09:00:00+0100",
      "active" : false
    }
  ],
  "page" : 1,
  "count" : 1,
  "pageSize" : 50
}
```

13.2.2 Create

To create a new scheduled Maintenance you need to send a Maintenance object without the attributes `id`, `created`, `modified`, and `active`. All those attributes are generated by the server and returned to you after a successful insert.

If your current time is between "start" and "end" date your maintenance page will be activated immediately!

To enqueue a maintenance page for all subdomains you have to use the `ALL:domain` annotation as `fqdn`.

```
PUT /{language}/rapi/maintenance/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "fqdn" : "www.example.com",
  "content" : "<html>Your maintenance page</html>",
  "start" : "2014-09-01T00:00:00+0200",
  "end" : "2014-09-01T09:00:00+0200"
}
```

If you prefer a default page from Myra you can do that by sending the following request:

```
PUT /{language}/rapi/maintenance/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "fqdn" : "www.example.com",
  "start" : "2014-09-01T00:00:00+0200",
  "end" : "2014-09-01T09:00:00+0200",
  "defaultPage" : {
    "facebook" : "URL",
    "twitter" : "URL",
    "custom" : {
      "label" : "label",
      "url" : "URL"
    }
  }
}
```

You can also reference an already existing maintenance page to reuse its content instead of sending the content in the request:

```
PUT /{language}/rapi/maintenance/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "fqdn" : "www.example.com",
  "start" : "2014-09-01T00:00:00+0200",
  "end" : "2014-09-01T09:00:00+0200",
  "contentFrom" : "test.domain.de"
}
```

A successful insert will return a ResultVO with the newly created Maintenance returned as targetObject. The response will also show whether the new maintenance was instantly activated by the API. When you use a default page instead of using your own, the default page will be returned in the `content` attribute. All attributes including `defaultPage` are optional. Custom link is only usable when using `custom.label` and `custom.url` together.

```
{
  "error" : false,
  "violationList" : [],
  "targetObject" : [
    {
      "id" : 1,
      "modified" : "2014-03-06T18:21:49+0100",
      "created" : "2014-03-06T18:21:49+0100",
      "fqdn" : "www.example.com",
      "start" : "2014-09-01T00:00:00+0200",
      "end" : "2014-09-01T09:00:00+0200",
      "content" : "<html>Maintenance page</html>",
      "active" : false
    }
  ]
}
```

13.2.3 Update

Updating a Maintenance is very similar to create a new one. The main difference is that an update will need the `id` and `modified` attributes to identify the version of the object you are trying to update.

```
POST /{language}/rapi/maintenance/{domain} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
{
  "id" : 3,
  "fqdn" : "www.example.com",
  "modified" : "2013-12-09T11:30:00+0100",
  "start" : "2014-09-04T00:00:00+0100",
  "end" : "2014-09-04T09:00:00+0100",
  "content" : "<html>Maintenance page</html>"
}
```

To see a valid response, take a look at the response from the create section. After an update your configuration will be queued and deployed to our system.

13.2.4 Delete

If the maintenance page you are going to delete is active, then it will be automatically disabled and the website will not be in maintenance mode anymore!

To delete a maintenance you just need to send only `id` and `fqdn` as body content.

```
DELETE /{language}/rapi/maintenance/{domain} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
{
  "id" : 3,
  "fqdn" : "www.example.com"
}
```

After a delete operation is done your configuration will be queued and deployed to our system.

13.3 Full version of a Maintenance object

Twitter has changed its name to X but in Myra defaultPage we still use the placeholder twitter.

```
{
  "id" : 1,
  "modified" : "2013-12-11T11:35:00+0100",
  "created" : "2013-12-09T11:35:00+0100",
  "fqdn" : "subdomain.example.de",
  "start" : "2014-08-27T09:00:00+0100",
  "end" : "2014-08-27T18:00:00+0100",
  "content" : "<html>content</html>",
  "active" : true,
  "defaultPage" : {
    "twitter" : "URL",
    "facebook" : "URL",
    "custom" : {
      "label" : "label",
      "url" : "URL"
    }
  }
}
```

Attribute name	Short description	Type	Supported methods	Required
id	Id of the object	Number	Update, Delete	Yes
modified	Date of last modification	Date	Update	Yes
created	Date of creation	Date	-	No
fqdn	Subdomain name for a maintenance entry	String	Create, Update	Yes
start	Date of maintenance to start	Date	Create, Update	No
end	Date of maintenance to end	Date	Create, Update	No
content	HTML content to show when maintenance is active	String	Create, Update	Optional
contentFrom	Use content of maintenance page from the given fqdn	String	Create	Optional
active	Shows if a maintenance is currently active	Boolean	Create, Update	Optional

Attribute name	Short description	Type	Supported methods	Required
defaultPage	Allows to append urls for Twitter/X and Facebook used by the generated default page, or other custom placeholders in the template	Object	Create, Update	Optional
id	Id is an unique identifier for an object. This value is always a number type and cannot be set, while inserting a new object. To update or delete a Maintenance it is necessary to add this attribute to your object.			
modified	Identifies the version of the object. To ensure that you are updating the most recent version and not overwriting other changes, you always have to add modified for updates and deletions. This value is always a date type with an ISO 8601 format.			
created	Created is a date type attribute with an ISO 8601 format. It will be created by the server after creating a new Maintenance object. This value is only informational so it is not necessary to add this an attribute to any API call.			
fqdn	Shows a FQDN (fully qualified domain name) for a maintenance. This attribute shows the domain to handle maintenance for.			
start	Start is a date type attribute with an ISO 8601. This attribute shows the start date for a maintenance. This date have to be lower than end or null to start now.			
end	End is a date type attribute with an ISO 8601 and shows the end date for a maintenance. This date have to be higher than start or null to end now.			
content	HTML content to show as maintenance page. Please note that it is not possible to include resources from the domain you have set to maintenance mode. If your maintenance page contains images use a different domain or use inline base64 encoded images.			
contentFrom	This property can be used instead of the property content to reference an existing maintenance page's content. Instead of sending the actual content, specify a valid FQDN here. This will copy the content from the referenced maintenance page to the newly created.			
active	This information shows if this a maintenance page is currently active. You cannot set this attribute directly instead you have to set start and end attribute to activate maintenance.			

defaultPage This allows an API user to set a maintenance with a default page generated by Myra. To append customer specific parts (Facebook and Twitter/X) you can append this keys to the given object and set an URL to the specific service. Both URLs can be used simultaneously. The `defaultPage` option also allows you to set a customer specific link on the generated page using the custom field, with providing custom placeholders in the generated file.

14 SSL certificates

14.1 Overview

This endpoint lets you manage your SSL certificates.

14.2 Usage

All SSL requests use URL specific parameters. A list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	String	Yes	The domain you are working on.
page	Number	Yes	Number of the page you want to retrieve (1-based).

14.2.1 Listing

To list all SSL certificates that belong to a given domain, you have to use the following REST request:

```
GET /{language}/rapi/certificates/{domain}/{page} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```

A successful call will return a response with a HTTP status code of 200 and the following body:


```
{
  "error":false,
  "list":[
    {
      "objectType":"SslCertV0",
      "id":98765,
      "modified":"2016-06-28T15:33:25+0200",
      "created":"2016-06-28T15:33:25+0200",
      "subject":"OU=Domain Control Validated Free SSL, CN=myracloud.com",
      "algorithm":"RSA-SHA1",
      "validFrom":"2012-10-18T00:00:00+0000",
      "validTo":"2013-01-16T23:59:59+0000",
      "fingerprint":"7A:E6:79:37:42:08:EF:12:D2:38:B0:EE:E3:1F:C5...",
      "serialNumber":"58:B8:3F:43:98:56:79:35:90:E9:6C:41:30:F1:7D:0D",
      "managed": false,
      "password": "",
      "subjectAlternatives":[
        "myracloud.com",
        "www.myracloud.com"
      ],
      "intermediates":[
        {
          "objectType":"SslIntermediateV0",
          "subject":"C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=...",
          "algorithm":"RSA-SHA1",
          "validFrom":"2006-12-01T00:00:00+0000",
          "validTo":"2020-05-30T10:48:38+0000",
          "fingerprint":"59:99:9D:FD:06:B3:CB:1F:73:D6:6A:81:D5:51:B0...",
          "serialNumber":"2E:79:83:2E:90:88:87:EA:8B:8E:F3:1A:6E:E6:7A:44",
          "issuer":"C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=..."
        },
        {
          "objectType":"SslIntermediateV0",
          "subject":"C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=...",
          "algorithm":"RSA-SHA1",
          "validFrom":"2005-06-07T08:09:10+0000",
          "validTo":"2020-05-30T10:48:38+0000",
          "fingerprint":"21:3F:AD:03:B1:C5:23:47:E9:A8:0F:29:9A:F0:89...",
          "serialNumber":"46:EA:F0:96:05:4C:C5:E3:FA:65:EA:6E:9F:42:C6:64",
          "issuer":"C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=..."
        }
      ],
      "wildcard":false,
      "extendedValidation":false,
      "subdomains":[
        "www.myracloud.com"
      ]
    }
  ],
  "page":1,
  "count":1,
  "pageSize":50
}
```

14.2.2 Create

To upload and assign a new certificate send a SslCertVO object without the attributes `id`, `created`, and `modified`. All attributes are generated by the server and will be returned after that.

```
PUT /{language}/rapi/certificates/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "objectType":"SslCertVO",
  "cert": "(( certificate ))",
  "certRefreshForce":false,
  "certToRefresh":54321,
  "intermediates":[
    {
      "cert": "(( intermediate certificate or chain of certificates (PEM) ))"
    }
  ],
  "key": "(( private key ))",
  "subdomains":[
    "www.myracloud.com",
    "www2.myracloud.com"
  ]
}
```

A successful insert will return a ResultVO with the assigned subdomains and intermediates. Please note that the API will never return the certificate nor the private key.

After a successful upload your configuration will be queued and deployed to our system.

14.2.3 Refreshing existing certificates

The Myra API supports an option to refresh existing certificates while retaining the current IP addresses. To achieve this, you should use the CREATE endpoint, just like when creating a new certificate, but with the `certToRefresh` property set to the id of the existing certificate you want to refresh:

```
PUT /{language}/rapi/certificates/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "objectType": "SslCertV0",
  "cert": "(( certificate ))",
  "certRefreshForce": false,
  "certToRefresh": 54321,
  "intermediates": [
    {
      "cert": "(( intermediate certificate or chain of certificates (PEM) ))"
    }
  ],
  "key": "(( private key ))",
  "subdomains": [
    "www.myracloud.com",
    "www2.myracloud.com"
  ]
}
```

14.2.4 Update

When updating a certificate, **the API does not allow you to change the certificate or the key**. If you would like to do so, **you need to upload the certificate again**. However, it is possible to change the intermediate chain as well as the assigned subdomains.

```
POST /{language}/rapi/certificates/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "id":3,
  "modified":"2013-12-09T11:30:00+0100",
  "intermediates":[
    {
      "cert":"(( intermediate or chain of intermediates (PEM) ))"
    }
  ],
  "subdomains":[
    "www3.myracloud.com"
  ]
}
```

To see an example of a valid response you can take a look at the response example in the create section.

After an update your configuration will be queued and deployed to our system.

14.2.5 Delete

It is not necessary to delete a certificate. When a certificate is found assigned to no sub-domain, for more than one week, it will be automatically removed.

14.3 Full version of a SslCertVO object

```
{
  "objectType": "SslCertVO",
  "cert": "(( certificate ))",
  "certRefreshForce": false,
  "certToRefresh": 54321,
  "intermediates": [
    {
      "cert": "(( intermediate certificate or chain of certificates (PEM) ))"
    }
  ],
  "key": "(( private key ))",
  "password": "",
  "subdomains": [
    "www.myracloud.com",
    "www2.myracloud.com"
  ]
}
```

```
{
  "objectType": "SslCertV0",
  "id": 12345,
  "modified": "2016-04-12T15:03:23+0200",
  "created": "2016-04-12T15:03:23+0200",
  "subject": "C=DE, O=Example certificate, ST=Bavaria, L=Munich, CN=myracloud.com",
  "algorithm": "RSA-SHA256",
  "validFrom": "2016-04-12T09:01:26+0200",
  "validTo": "2019-04-17T23:59:59+0200",
  "fingerprint": "43:51:A1:B5:FC:8B:B7:0a:3a:a9:b1:0f:66:73:a8:37:27:47:DD:EC:69:CA:31:71...",
  "serialNumber": "80:3D:33:8A:0E:FC:18:C4",
  "managed": false,
  "password": "",
  "subjectAlternatives": [
    "www.myracloud.com",
    "www2.myracloud.com"
  ],
  "intermediates": [
    {
      "objectType": "SslIntermediateV0",
      "subject": "C=SE, O=AddTrust AB, OU=AddTrust..., CN=AddTrust External CA Root",
      "algorithm": "RSA-SHA256",
      "validFrom": "2014-07-09T17:14:50+0200",
      "validTo": "2021-07-09T17:09:04+0200",
      "fingerprint": "49:F7:28:C0:0C:FC:F5:B4:43:D6:6D:E9:D3:81:1F:64:F8:29:B1:1D:8D:94...",
      "serialNumber": "72:7B:21:6",
      "issuer": "C=SE, O=AddTrust AB, OU=AddTrust..., CN=AddTrust External CA Root2"
    }
  ],
  "wildcard": false,
  "extendedValidation": false,
  "subdomains": [
    "www.myracloud.com",
    "www2.myracloud.com"
  ]
}
```

Attribute name	Short description	Type	Supported methods	Required
id	Id of the object	Integer	Update, Delete	Yes
modified	Date of last modification	Date	Update, Delete	Yes
created	Date of creation	Date	-	No
cert	Contains the certificate	String	Create	Yes
certRefreshForced	True to force certificate update	Boolean	Create	Yes

Attribute name	Short description	Type	Supported methods	Required
certToRefresh	Id of the certificate to refresh	Integer	Create	Yes
key	Unencrypted private key	String	Create	Yes
subject	Subject of the certificate	String	-	Optional
algorithm	Signature algorithm of the certificate	String	-	Optional
validFrom	Time when the certificate starts to be valid	Date	-	Optional
validTo	Time when the certificate expires	Date	-	Optional
fingerprint	RSA 256 fingerprint of the certificate	String	-	Optional
serialNumber	Serial number of the certificate	String	-	Optional
subjectAlternatives	Subdomain(s) the certificate is valid for	Array	-	Optional
intermediates	An array of intermediate certificate(s)	Array	-	Optional
wildcard	True if the certificate contains a wildcard domain	Boolean	-	Optional
extendedValidation	True if the certificate has extended validation	Boolean	-	Optional
subdomains	List of subdomains assigned to this certificate	Array	Create	Yes
managed	True if the certificate is managed by Myra	Boolean	-	Optional
password	Decrypt an encrypted SSL certificate	String	Create	Optional

id

Id is an unique identifier for an object. This value is always a number type and cannot be set while inserting a new object. To update or delete a cache setting it is necessary to add this attribute to your object.

modified

Identifies the version of the object. To ensure that you are updating the most recent version and not overwriting other changes, you always have to add the modified timestamp for updates and deletes. This value is always a date type with an ISO 8601 format.

created	Created is a date type attribute with an ISO 8601 format. It will be created by the server after creating a new cache setting object. This value is only informational so it is not necessary to add this attribute to every API call.
cert	Cert contains the certificate.
certRefreshForced	Every time a certificate is refreshed with another non-matching certificate the operation is interrupted with an error. Setting <code>certRefreshForced</code> will ignore such errors and refresh the certificate anyway. Please use it only, if you are sure you can ignore an error when refreshing a certificate.
certToRefresh	This property allows you to update an already existing certificate with a new one without changing IP addresses.
key	The unencrypted private key that matches your certificate.
subject	Shows the subject of the uploaded certificate.
algorithm	Contains the signature algorithm.
validFrom	Time when the certificate starts to be valid. This property is a date type with an ISO 8601 format.
validTo	Time when the certificate expires. This property is a date type with an ISO 8601 format.
fingerprint	Fingerprint of the certificate.
serialNumber	Serial number of the certificate.
subjectAlternatives	Contains a list of subdomains which can be validated using this certificate. This list also contains the CN of the subject.
intermediates	Contains a list of intermediate certificates to be used in order to generate a chain of trust. The intermediates are filtered and sorted based on subject / issuer relationship. Uploading a partial or a completely different chain will result in an empty list. When returned, the list contains a set of <code>SslIntermediateVO</code> objects.
wildcard	This property shows whether the certificate is valid for multiple subdomains of a domain. The certificate needs to have a *.domain.tld subject to return true.
extendedValidation	True if the browser handles the certificate as extended validation. We use the OIDs from Google Chrome™ to measure the extended validation level.

subdomains	A list of subdomains assigned to this certificate.
managed	True if the certificate is managed by Myra. In that case, the certificate is not editable via API, it can only be read. The value of this field cannot be set when creating/updating a certificate via API.
password	This field will be used to decrypt an encrypted SSL certificate. An Encrypted SSL certificate should be under the PKCS12 specification format. In such a case, the cert field should then contain a base64 encoded value of the binary encrypted certificate (as it is not possible to set a binary content in a JSON field). The password field will be ignored if the content of the cert field isn't an PKCS12 format.

15 Statistics

15.1 Overview

The statistics API lets you fetch statistical data of your domains like requests, traffic, performance, or health.

15.2 Usage

All static requests use URL specific parameters; a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.

15.2.1 Query

To fetch statistical data of your domains, you can use the following REST request:

```
POST /{language}/rapi/statistic/query HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "query": {
    "aggregationInterval": "hour",
    "dataSources" : {
      "myDataSource": {
        "source": "bytes_cache_hits",
        "type" : "stats"
      }
    },
    "startDate" : "2015-01-27T00:00:00+0100",
    "endDate" : "2015-01-27T12:00:59+0100",
    "fqdn" : [
      "ALL:example.com"
    ],
    "type" : "fqdn"
  }
}
```

A successful call will return the original query and the actual result as an object with the key `result`. For each data source given in the query a result set will be returned with the same name.

```
{
  "query" : {
    "aggregationInterval": "hour",
    "dataSources" : {
      "myDataSource": {
        "source": "bytes_cache_hits",
        "type" : "stats"
      }
    },
    "startDate" : "2015-01-27T00:00:00+0100",
    "endDate" : "2015-01-27T12:00:59+0100",
    "fqdn" : [
      "ALL:example.com"
    ],
    "type" : "fqdn"
  },
  "result": {
    "myDataSource" : {
      "avg": 5866621.8906448,
      "max": 65366760,
      "min": 0,
      "sum": 18561991662
    },
    "requests_histogram": {
      "1422399600000": {
        "avg": 334.70860927152,
        "max": 1609,
        "min": 1,
        "sum": 101082
      }
    }
  }
}
```

15.3 StatisticVO

```
{
  "query" : {},
  "result": {}
}
```

Attribute name	Short description	Type	Supported methods	Required
query	Contains the StatisticQueryVO	Object	Request	Yes
result	Returns the detailed custom data for the requested domain	Object	-	No

query Information about the structure of \$query can be found in section 15.3.1. The given query object is returned unchanged in the response of the API call.

result The result object is ignored for requests and should be empty. It will contain the result of the query specified in the query.

15.3.1 StatisticQueryVO

```
{
  "aggregationInterval": "hour",
  "dataSources" : {
    "name": {
      "source": "bytes_cached",
      "type" : "stats"
    }
  },
  "startDate" : "2015-01-27T00:00:00+0100",
  "endDate" : "2015-01-27T12:00:59+0100",
  "fqdn" : [
    "www.example.com"
  ],
  "type" : "fqdn"
}
```

Attribute name	Short description	Type	Supported methods	Required
aggregationInterval	The interval for aggregating the data points	String	Request	Optional
dataSources	List of data sources and output type	Object	Request	Yes
startDate	Start of the aggregation interval	DateTime	Request	Yes
endDate	End of the aggregation interval	DateTime	Request	Yes
fqdn	A list of FQDN	Array	Request	Yes
type	Mode for selecting domains which should be used	String	Request	Optional

aggregationInterval The statistics can be requested in various aggregation intervals. The requested data will be split into buckets of the given date interval. This applies only to data requested as histogram. Default value: `day` Allowed values: `5m`, `hour`, `day`, `week`

dataSources Information about the structure can be found in section 15.3.2. At least one data source should be provided.

startDate Included start of the requested period. It should be in ISO 8601 format.
For example: `2015-03-13T12:00:00+01:00`. Allowed values: ISO 8601 format

endDate Included end of the requested period. It should be in ISO 8601 format.
For example: `2015-04-21T12:00:00+01:00`. Allowed values: ISO 8601 format

fqdn Contains a list of FQDN for which statistics should be generated. Note that you can also use `ALL:fqdn.de` as domain name to include data for all subdomains. This value is only used if the `$type` is set to `fqdn`. Allowed values: Normal fqdn, ALL notation domain

type Mode for selecting domains which should be used.
Default value: `fqdn` Allowed values: `fqdn`, `all`, `own`, `foreign`

15.3.2 Data sources

With the statistics API, you can query various information about request types and how they were handled.

```
{
  "nameExample": {
    "source": "bytes_cached",
    "type" : "stats"
  }
}
```

Attribute name	Short description	Type	Supported methods	Required
name	Arbitrary name of the dataset (can be named anything)	String	Request	Yes
source	Category of the requested data source	String	Request	Yes
type	Type of the data aggregation	String	Request	Yes

name The given name is used to name the corresponding result set in the API response. The name may only contain [a-zA-Z0-9_] characters.
Examples: requests_histogram, url_hits_top, cache_misses_top

source See the tables under the sections Requests, Traffic, or Other data sources with a list of possible data source names to use.

type The statistic data can be requested in two different aggregation types.

stats: Data as object containing min/max/avg/sum values.

histogram: Response will consist of multiple objects containing the value for every aggregation bucket. Allowed values: `stats`, `histogram`

15.3.2.1 Requests

Myra distinguishes incoming requests as SSL and non-SSL depending on the protocol used by the client initiating the request. You can also retrieve information about whether the response was sent from the Myra cache or from origin system.

Data source	S	N	C	U	Description
requests	X	X	X	X	Total amount of requests handled by Myra
requests_ssl	X		X	X	Amount of requests received via SSL
requests_nonssl		X	X	X	Amount of requests received not via SSL
requests_cached	X	X	X		Total amount of requests delivered from cache
requests_cached_ssl	X		X		Amount of requests via SSL delivered from cache
requests_cached_nonssl		X	X		Amount of requests via non-SSL delivered from cache
requests_uncached	X	X		X	Total amount of requests passed to the origin
requests_uncached_ssl	X			X	Total amount of requests via SSL passed to the origin
requests_uncached_nonssl		X		X	Total amount of requests via non-SSL passed to the origin
requests_cache_hits	X	X	X		Ratio of total cached requests to uncached requests in percent
requests_cache_hits_ssl	X		X		Ratio of SSL cached requests to SSL uncached requests in percent
requests_cache_hits_nonssl		X	X		Ratio of non-SSL cached requests to non-SSL uncached requests in percent

S = SSL, **N** = non-SSL, **C** = Cached, **U** = Uncached

Data source Name of the data source.

SSL Includes amount of requests sent and answered via SSL connection.

non-SSL Includes amount of requests sent and answered via non-SSL connection.

Cached Includes amount of requests answered from the Myra cache without querying the origin server.

Uncached Includes amount of requests answered by Myra after passing the request to the origin server and sending the corresponding response.

15.3.2.2 Traffic

Myra distinguishes transferred data as SSL and non-SSL traffic depending on the protocol used by the client initiating the request. You can also retrieve information about whether the response was sent from the Myra cache or was fetched from the origin system.

Data source	S	N	C	U	Description
bytes	X	X	X	X	Total amount of outgoing data in bytes
bytes_ssl	X		X	X	Amount of data sent via SSL
bytes_nonssl		X	X	X	Amount of data sent via non-SSL
bytes_cached	X	X	X		Total amount of data delivered from the cache
bytes_cached_ssl	X		X		Amount of data via SSL delivered from the cache
bytes_cached_nonssl		X	X		Amount of data via non-SSL delivered from the cache
bytes_uncached	X	X		X	Total amount of data passed through from the origin
bytes_uncached_ssl	X			X	Amount of data passed via SSL from the origin
bytes_uncached_nonssl		X		X	Amount of data passed via non-SSL from the origin
bytes_cache_hits	X	X	X		Ratio of total bytes delivered from the cache in percent
bytes_cache_hits_ssl	X		X		Ratio of bytes delivered via SSL from the cache in percent
bytes_cache_hits_nonssl		X	X		Ratio of bytes delivered via non-SSL from the cache in percent

S = SSL, **N** = non-SSL, **C** = Cached, **U** = Uncached

Data source Name of the data source.

SSL Includes bytes transferred via SSL connection.

non-SSL Includes bytes transferred via non-SSL connection.

Cached Includes bytes of all responses transferred from Myra cache without querying the origin server.

Uncached Includes bytes of all responses transferred from Myra without caching.

15.3.2.3 Other

In addition to traffic and request statistics, Myra allows you to view detailed information about geographic distribution of your visitors, the performance of your origin server and the HTTP response codes of your application.

Data source	S	N	C	U	Description
upstream_performance	X	X		X	Average upstream response time
response_codes	X	X	X	X	HTTP response codes of total requests
country_codes	X	X	X	X	Total requests by country

S = SSL, **N** = non-SLL, **C** = Cached, **U** = Uncached

15.3.3 Result

```
{
  "bytes_cached_stats": {
    "avg": 5866621.8906448,
    "max": 65366760,
    "min": 0,
    "sum": 18561991662
  },
  "requests_histogram": {
    "1422399600000": {
      "avg": 334.70860927152,
      "max": 1609,
      "min": 1,
      "sum": 101082
    }
  }
}
```

Attribute	Type	Description
name	String	Name of the result set according to chosen name in the request
avg	Float	The average value of the requested source
max	Float	The maximal value of the requested source
min	Float	The minimal value of the requested source
sum	Float	The sum of the requested source

The structure of the returned data depends on the requested type. Data sources requested with type `stats` will be returned as an object with min/max/avg/sum keys as seen in `bytes_cached_stats` above. Responses for type `histogram` will contain multiple objects with the key value, one object for every aggregation bucket. Please note that the **timestamp** used as key is **in milliseconds**.

16 IP address ranges of Myra

16.1 Overview

You can use the Myra IP address ranges as a whitelist on your firewall, to configure Real-IP in Nginx or mod_remoteip in Apache, or to restrict requests to only the Myra IP address ranges.

16.2 Usage

All IP address ranges (networks) requests use URL specific parameters, a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.

16.2.1 Listing

The listing operation returns a list of IP address ranges. The list contains Myra's IPv4 and IPv6 address ranges which are used to connect to your system.

The REST request must have the following format:

```
GET /{language}/rapi/networks HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
```

A successful call will return a response with a HTTP status code of 200 and the following body:

```
{
  "error": false,
  "list": [
    {
      "id": 37,
      "modified": "2018-10-15T21:49:41+0200",
      "created": "2018-06-25T13:27:06+0200",
      "network": "103.51.165.0/24",
      "enabled": true,
      "validFrom": "2018-06-25T02:00:00+0200"
    },
    ...
  ],
  "page": 1,
  "count": 29,
  "pageSize": 50
}
```

16.2.2 Create

Creating a new IP address range is not possible.

16.2.3 Update

Updating IP address ranges is not possible.

16.2.4 Delete

Deleting IP address ranges is not possible.

16.3 Full version of a IP address range object

```
{
  "id": 37,
  "modified": "2018-10-15T21:49:41+0200",
  "created": "2018-06-25T13:27:06+0200",
  "network": "103.51.165.0/24",
  "enabled": true,
  "validFrom": "2018-06-25T02:00:00+0200"
}
```

Attribute name	Description	Method type
id	Id is an unique identifier for an object. This value is always a number	Number
modified	Identifies the version of the object. This value is always a date type with an ISO 8601 format	Date
created	Created is a date type attribute with an ISO 8601 format	Date
network	Network contains the IP address range in CIDR notation	String
enabled	Enabled shows whether this entry is valid or invalid	Boolean
validFrom	ValidFrom gives information about from which date on the IP address range is valid in ISO 8601 format	Date

17 Error Pages

17.1 Overview

The error page functionality allows you to set an error page which is directly served from Myra servers.

17.2 Usage

All error page requests use URL specific parameters, a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	String	Yes	The domain you are trying to list error pages for.
page	Number	Yes	Number of the page you want to retrieve (1-based).

17.2.1 Listing

To reduce the size of the response, the listing request will not return the content of the error pages.

To list all error pages belonging to a given domain you have to use the following REST request:

```
GET /{language}/rapi/errorpages/{domain}/{page} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```

A successful call will return a response with a HTTP status code 200 and the following body:

```
{
  "error": false,
  "violationList": [],
  "warningList": [],
  "page": 1,
  "count": 1,
  "pageSize": 10,
  "list": [
    {
      "subDomainName": "www.example.com",
      "error": {
        "503": {
          "errorCode": 503,
          "content": "",
          "id": 1,
          "modified": "2023-09-04T13:12:42+0200",
          "created": "2023-09-04T13:12:42+0200"
        }
      }
    }
  ]
}
```

17.2.2 Fetching

To get a single error page you have to use the following REST request:

```
GET /{language}/rapi/errorpage/{id} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```

A successful call will return a response with a HTTP status 200 and the following body:

```
{
  "error": false,
  "violationList": [],
  "warningList": [],
  "list": [
    {
      "subDomainName": "www.example.com",
      "error": {
        "503": {
          "errorCode": 503,
          "content": "<html><body> error page 503 </body></html>",
          "id": 1,
          "modified": "2023-09-04T13:12:42+0200",
          "created": "2023-09-04T13:12:42+0200"
        }
      }
    }
  ],
  "pageSize": 10,
  "page": 0,
  "count": 1
}
```

17.2.3 Create

To create a global error page for the full domain you can use the ALL-domainId notation.

To create a new error page entry you have to send a request with this JSON structure:

```
POST /{language}/rapi/errorpages/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "pageContent": "<html><body>Error page 500</body></html>",
  "selection": {
    "www.example.com": {
      "500": true,
      "503": true
    },
    "ALL-{domainId}": {
      "500": true
    }
  }
}
```

17.2.4 Update

It is not possible to update an error page, but you can call the create request again with different pageContent, which will replace the old error page with the new one.

17.2.5 Delete

To delete an error page entry you have to send a request with this JSON structure:

```
DELETE /{language}/rapi/errorpages/{domain} HTTP/1.1
Host: api.myracloud.com
Date: 2014-06-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
{
  "selection": {
    "www.example.com": {
      "503": true
    },
    "ALL-{domainId}": {
      "500": true
    }
  }
}
```

17.3 Structure of the request JSON

Attribute name	Description	Method type
pageContent	The HTML content of the error page	String
selection	You can add a list of subdomains, and inside the subdomain you can set the error code with a boolean value. When the boolean value is <code>true</code> the error page for this subdomain and error code will be created, updated, or deleted	Object

17.4 Full version of an error page object

```
{
  "id": 1,
  "modified": "2023-09-04T13:12:42+0200",
  "created": "2023-09-04T13:12:42+0200",
  "errorCode": 503,
  "content": "<html><body>Error page 503</body></html>"
}
```

Attribute name	Description	Method type
id	Id is an unique identifier for an object. This value is always a number	Number
modified	Identifies the version of the object. This value is always a date type with an ISO 8601 format	Date
created	Created is a date type attribute with an ISO 8601 format	Date
errorCode	HTTP status code of the error page	Integer
content	HTML content of the error page	String

18 Rate Limit

18.1 Overview

The rate limit functionality allows you to set rate limits for specific IP ranges.

18.2 Usage

All rate limit requests use URL specific parameters, a list of these parameters can be found in the table below.

Parameter	Type	Required	Description
language	String	Yes	Sets the preferred language of the error messages. Valid values are currently only <code>en</code> for English or <code>de</code> for German.
domain	String	Yes	The domain you are trying to list error pages for.
page	Number	Yes	Number of the page you want to retrieve (1-based).

18.2.1 Listing

To get a list of IP rate limit object belonging to your given domain you have to use the following REST request:

```
GET /{language}/rapi/ratelimit/dns/{page}?subDomainName={subDomainName} HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
```

A successful call will return a response with a HTTP status of 200 and the following body:

```
{
  "error": false,
  "violationList": [],
  "warningList": [],
  "page": 1,
  "count": 1,
  "pageSize": 50,
  "list": [
    {
      "network": "192.168.2.2/32",
      "value": 60,
      "burst": 50,
      "timeframe": 120,
      "subDomainName": "www.example.com.",
      "id": 1,
      "modified": "2023-10-05T12:51:13+0200",
      "created": "2023-10-05T12:51:13+0200"
    }
  ]
}
```

18.2.2 Create

To create a global rate limit for the full domain you can use the ALL-domainId notation in subDomainName field.

To create a new IP rate limit entry you have to send a RateLimit object without the `id`, `created`, and `modified` attributes. All these attributes are generated by the server and returned after that.

```
PUT /{language}/rapi/ratelimit HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
{
  "subDomainName": "www.example.com",
  "network": "192.168.2.2/32",
  "value": 60,
  "burst": 50,
  "timeframe": 120
}
```

A successful insert will return a ResultVO with the newly created RateLimit.

```
{
  "error": false,
  "violationList": [],
  "warningList": [],
  "targetObject": [
    {
      "network": "192.168.2.2/32",
      "value": 60,
      "burst": 50,
      "timeframe": 120,
      "subDomainName": "www.example.com.",
      "id": 1,
      "modified": "2023-10-05T12:51:13+0200",
      "created": "2023-10-05T12:51:13+0200"
    }
  ]
}
```

18.2.3 Update

Updating a rate limit is very similar to creating a new one. You will need to provide the generated `id` and `modified` attributes to identify the version of the object you are trying to update.

```
POST /{language}/rapi/ratelimit HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
{
  "id": 1,
  "modified": "2023-10-05T12:51:13+0200",
  "subDomainName": "www.example.com",
  "network": "192.168.1.2/32",
  "value": 60,
  "burst": 50,
  "timeframe": 120
}
```

To see a valid response, take a look at the response from the create section.

After an update your configuration will be queued and deployed to our system.

18.2.4 Delete

To delete a rate limit record it is just necessary to send only `id` and `subDomainName` as body content.

```
DELETE /{language}/rapi/ratelimit HTTP/1.1
Host: api.myracloud.com
Authorization: MYRA {apiKey}:{signature}
Date: 2014-05-02T07:17+0200
{
  "id": 1,
  "subDomainName": "www.example.com"
}
```

After a delete operation your configuration will be queued and deployed to our system.

18.3 Full version of rate limit object

Attribute name	Short description	Type	Supported methods	Required
id	Id of the object	Integer	Update, Delete	Yes
modified	Date of last modification in ISO 8601 format	Date	Update	Yes
created	Date of creation in ISO 8601 format	Date	-	No
subDomainName	Subdomain name of a rate limit	String	Create, Update	Yes
network	Network in CIDR notation affected by the rate limiter	String	Create, Update	Yes
value	Maximum amount of requests for the given network. Valid values are: 0 , 60 , 100 , 500 , 1000 , 2000 , 4000	Integer	Create, Update	Yes
burst	Burst defines how many requests a client can make in excess of the specified rate.	Integer	Create, Update	Yes
timeframe	The affected timeframe in seconds for the rate limit. Valid values are: 1 , 2 , 5 , 10 , 15 , 30 , 45 , 60 , 120 , 180 , 300 , 600 , 1200 , 3600	Integer	Create, Update	Yes

19 Bind zone file endpoints

Bind zone endpoint is used to fetch bind zone either as a file or as a JSON data. Both endpoints are GET requests and can only be accessed by users that belong to the root group of an organization. For this, there are two different endpoints:

19.1 Raw bind zone

The raw bind zone endpoint returns the *text/plain* content type. It outputs the content of the configuration created for it.

Example request for the domain myracloud.com

```
GET /{language}/rapi/bindRaw/{domainName} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```

Example response

```
$ttl 38400
test.de. IN SOA a.myradns.de. support.myrasecurity.com. (
    2693399977
    16384
    2048
    1048576
    2560 )
test.de. IN NS a.myradns.de.
test.de. IN NS b.myradns.de.
test.de. IN NS c.myradns.de.
test.de. 300 IN A 1.1.1.1
```

19.2 JSON bind zone

The JSON bind zone endpoint returns a JSON representation of the bind zone.

Example request for the domain myracloud.com

```
GET /{language}/rapi/bind/{domainName} HTTP/1.1
Host: api.myracloud.com
Date: 2014-05-02T07:17+0200
Authorization: MYRA {apiKey}:{signature}
```


Example response

```
{
  "error": false,
  "violationList": [

  ],
  "warningList": [

  ],
  "list": [
    {
      "objectType": "DomainBindV0",
      "domainName": "test.de",
      "ttl": 38400,
      "primaryDns": "a.myradns.de",
      "hostmaster": "support.myrasecurity.com",
      "timeToRefresh": 16384,
      "timeToRetry": 2048,
      "timeToExpire": 1048576,
      "minimumTTL": 2560,
      "version": 2693813617,
      "records": [
        {
          "domain": "test.de",
          "type": "NS",
          "value": "a.myradns.de.",
          "rtype": "dns"
        },
        {
          "domain": "test.de",
          "type": "NS",
          "value": "b.myradns.de.",
          "rtype": "dns"
        },
        {
          "domain": "test.de",
          "type": "NS",
          "value": "c.myradns.de.",
          "rtype": "dns"
        },
        {
          "domain": "test.de",
          "ttl": 300,
          "type": "A",
          "value": "1.1.1.1",
          "rtype": "record",
          "active": false
        }
      ]
    }
  ]
}
```

active	A boolean value indicating whether this DNS record is protected by Myra (<code>true</code>) or not (<code>false</code>).
type	This value shows the type of the DNS record. All available record types are <code>A</code> , <code>AAAA</code> , <code>MX</code> , <code>CNAME</code> , <code>TXT</code> , <code>NS</code> , <code>SRV</code> and <code>PTR</code> .
ttl	Time to live (ttl) is a numeric value and is given in seconds. If the record is protected by Myra, the ttl is always <code>300</code> .
value	If the DNS record is protected by Myra, the value is always the Myra IP. Otherwise, the IP is set by a user.
rtype	If the type of the DNS record is <code>NS</code> , the rtype is <code>dns</code> , otherwise it is <code>record</code> .
cnameAlt	This value is only present if the DNS record is protected by Myra.

20 Interaction with Myra Web API

Using HashiCorp's "Infrastructure as Code" tool Terraform or our Go client are easy ways to communicate and interact with the Myra Web API.

20.1 Terraform Provider

With our Terraform Provider, you can configure and manage Myra elements and configurations in source code. Like this, it is easily possible to track and version your changes and – if necessary – do a rollback to some previous state.

You can find our Terraform Provider and more information here:

<https://github.com/Myra-Security-GmbH/terraform-provider-myrasec>

For the Myra Security Terraform Provider documentation, see here:

<https://github.com/Myra-Security-GmbH/terraform-provider-documentation>

20.2 Go client

With our Go client, you can interact with the Myra Web API.

You can find our Go client "myrasec-go" and more information here:

<https://github.com/Myra-Security-GmbH/myrasec-go>

Please note: Our Terraform Provider and Go client are both still under development and do not yet support all Myra Web API features. If you need the full API functionality, please use the Myra Web API directly.

21 Development

21.1 MYRA_NOCACHE

While a developer is working on a new feature or testing Myra's behavior, it is sometimes necessary to prevent the caching layer from doing its work. To prevent Myra from caching your request(s) you have to set a cookie on your domain with `MYRA_NOCACHE=1`. Now all your requests targeting the cookie domain are responded from your origin server.

